National Infrastructure Protection Plan

2006

Homeland Security

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
National Infrastructure Protection Plan	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Department of Homeland Security,Washington,DC,20528**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**196**	

Preface

Michael Chertoff
Secretary
Department of Homeland Security

The ability to protect the critical infrastructure and key resources (CI/KR) of the United States is vital to our national security, public health and safety, economic vitality, and way of life. U.S. policy focuses on the importance of enhancing CI/KR protection to ensure that essential governmental missions, public services, and economic functions are maintained in the event of a terrorist attack, natural disaster, or other type of incident, and that elements of CI/KR are not exploited for use as weapons of mass destruction against our people or institutions.

The President directed me to coordinate and implement national initiatives and develop a national plan to unify and enhance CI/KR protection efforts through an unprecedented partnership involving the private sector, as well as Federal, State, local, and tribal governments. The National Infrastructure Protection Plan (NIPP) meets the requirements that the President set forth in Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, and provides the overarching approach for integrating the Nation's many CI/KR protection initiatives into a single national effort.

The NIPP provides the coordinated approach that will be used to establish national priorities, goals, and requirements for CI/KR protection so that Federal funding and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. It establishes the overarching concepts relevant to all CI/KR sectors identified in HSPD-7, and addresses the physical, cyber, and human considerations required for effective implementation of comprehensive programs. The plan specifies the key initiatives, milestones, and metrics required to achieve the Nation's CI/KR protection mission. It sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for the Department of Homeland Security; Federal Sector-Specific Agencies; and other Federal, State, local, tribal, and private sector security partners.

The NIPP was developed through extensive coordination with security partners at all levels of government and the private sector. The processes described herein can be adapted and tailored to sector and individual security partner requirements. Participation in the implementation of the NIPP provides the government

and the private sector the opportunity to use collective expertise and experience to more clearly define CI/KR protection issues and practical solutions and to ensure that existing CI/KR protection planning efforts, including business continuity and resiliency planning, are recognized.

Continued cooperation and collaboration between and among these security partners is critical to the successful implementation of this plan. The NIPP provides specific implementation guidance for Federal departments and agencies and implementation recommendations for other security partners. I ask for your continued commitment and cooperation as we move forward to develop and implement the sector-specific aspects of the NIPP and enhance the protection of the Nation's CI/KR.

Michael Chertoff
Secretary
Department of Homeland Security

Letter of Agreement

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of critical infrastructure and key resources (CI/KR) protection into a single national program. The NIPP provides an overall framework for programs and activities that are currently underway in the various sectors, as well as new and developing CI/KR protection efforts. This collaborative effort between the private sector; State, Territorial, local, and tribal governments; nongovernmental organizations; and the Federal Government will result in the prioritization of protection initiatives and investments across sectors. It also will ensure that resources are applied where they offer the most benefit for mitigating risk by lowering vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other incidents. By signing this letter of agreement, Sector-Specific Agencies and other Federal departments and agencies with special functions related to CI/KR protection, as designated in Homeland Security Presidential Directive 7 (HSPD-7), commit to:

- Support NIPP concepts, frameworks, and processes, and carry out their assigned functional responsibilities as appropriate and consistent with their own agency-specific authorities, resources, and programs regarding the protection of CI/KR as described herein;
- Work with the Secretary of Homeland Security, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to coordinate funding and implementation of programs that enhance CI/KR protection;
- Provide annual reports, consistent with HSPD-7 requirements, to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors;
- Coordinate development of Sector-Specific Plans (SSPs) in collaboration with security partners and submit completed SSPs to the Department of Homeland Security within 180 days of final approval of the NIPP. Each SSP will align with the NIPP risk management framework and include a menu of sector-specific protective activities and a description of the sector's information-sharing mechanisms and protocols;
- Undertake the initiatives and actions outlined in the NIPP Initial Implementation Initiatives and Actions matrix in appendix 2B of this plan;

- Develop or modify existing interagency and agency-specific CI/KR plans, as appropriate, to facilitate compliance with the NIPP and SSPs;
- Develop and maintain partnerships for CI/KR protection with appropriate State, regional, local, tribal, and international entities; the private sector; and nongovernmental organizations as described herein; and
- Protect critical infrastructure information according to the Protected Critical Infrastructure Information program or other appropriate guidelines, and share information relevant to CI/KR protection (e.g., actionable information on threats, incidents, CI/KR status, etc.) as appropriate and consistent with their own agency-specific authorities and the processes described herein.

Signatory departments and agencies follow.

Signatories

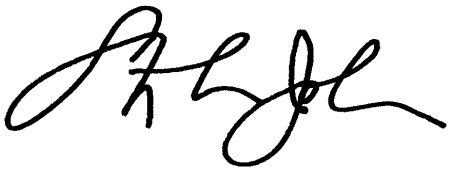
Mike Johanns
Secretary
Department of Agriculture

Carlos M. Gutierrez
Secretary
Department of Commerce

Donald H. Rumsfeld
Secretary
Department of Defense

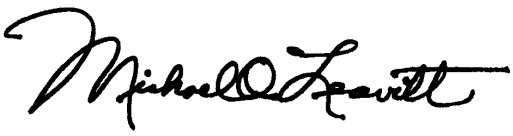
Margaret Spellings
Secretary
Department of Education

Samuel W. Bodman
Secretary
Department of Energy



Stephen L. Johnson
Administrator
Environmental Protection Agency

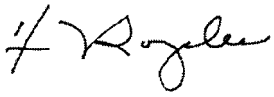
Robert S. Mueller, III
Director
Federal Bureau of Investigation



Michael O. Leavitt
Secretary
Department of Health and Human Services

Michael Chertoff
Secretary
Department of Homeland Security

P. Lynn Scarlett
Acting Secretary
Department of the Interior



Alberto R. Gonzales
Attorney General
Department of Justice

Nils Diaz
Chairman
Nuclear Regulatory Commission

Condoleezza Rice
Secretary
Department of State

Maria Cino
Deputy Secretary
Department of Transportation

John W. Snow
Secretary
Department of the Treasury

Table of Contents

Appendixes

List of Figures and Tables

Figures

Tables

Executive Summary

Protecting the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. Attacks on CI/KR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the Nation's CI/KR as weapons of mass destruction could have even more devastating physical and psychological consequences.

1 Introduction

The overarching goal of the National Infrastructure Protection Plan (NIPP) is to:

> ***Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.***

The NIPP provides the unifying structure for the integration of existing and future CI/KR protection efforts into a single national program to achieve this goal. The NIPP framework will enable the prioritization of protection initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters. The NIPP risk management framework recognizes and builds on existing protective programs and initiatives.

Protection includes actions to mitigate the overall risk to CI/KR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident (see figure S-1). Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety programs, and implementing cyber security measures, among various others.

More information about the NIPP is available on the Internet at:
www.dhs.gov/nipp or by contacting DHS at: **nipp@dhs.gov**

Figure S-1: Protection

Achieving the NIPP goal requires actions to address a series of objectives that include:

- Understanding and sharing information about terrorist threats and other hazards;
- Building security partnerships to share information and implement CI/KR protection programs;
- Implementing a long-term risk management program; and
- Maximizing efficient use of resources for CI/KR protection.

These objectives require a collaborative partnership between and among a diverse set of security partners, including the Federal Government; State, Territorial, local, and tribal governments; the private sector; international entities; and nongovernmental organizations. The NIPP provides the framework that defines the processes and mechanisms that these security partners will use to develop and implement the national program to protect CI/KR across all sectors over the long term.

2 Authorities, Roles, and Responsibilities

The Homeland Security Act of 2002 provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's CI/KR. The act assigns DHS the responsibility to develop a comprehensive national plan for securing CI/KR and for recommending "measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities."

The national approach for CI/KR protection is provided through the unifying framework established in Homeland Security Presidential Directive 7 (HSPD-7). This directive establishes the U.S. policy for "enhancing protection of the Nation's CI/KR" and mandates a national plan to actuate that policy. In HSPD-7, the President designates the Secretary of Homeland Security as the "principal Federal official to lead CI/KR protection efforts among Federal departments and agencies, State and local governments, and the private sector" and assigns responsibility for CI/KR sectors to specific Sector-Specific Agencies (SSAs) (see table S-1). In accordance with HSPD-7, the NIPP delineates roles and responsibilities for security partners in carrying out CI/KR protection activities while respecting and integrating the authorities, jurisdictions, and prerogatives of these security partners.

Primary roles for CI/KR security partners include:

- **Department of Homeland Security:** Manage the Nation's overall CI/KR protection framework and oversee NIPP development and implementation.
- **Sector-Specific Agencies:** Implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CI/KR sectors designated in HSPD-7.
- **Other Federal Departments, Agencies, and Offices:** Implement specific CI/KR protection roles designated in HSPD-7 or other relevant statutes, executive orders, and policy directives.
- **State, Local, and Tribal Governments:** Develop and implement a CI/KR protection program as a component of their overarching homeland security programs.
- **Regional Partners:** Use partnerships that cross jurisdictional and sector boundaries to address CI/KR protection within a defined geographical area.
- **Boards, Commissions, Authorities, Councils, and Other Entities:** Perform regulatory, advisory, policy, or business oversight functions related to various aspects of CI/KR operations and protection within and across sectors and jurisdictions.
- **Private Sector Owners and Operators:** Undertake CI/KR protection, restoration, coordination, and cooperation activities, and provide advice, recommendations, and subject matter expertise to the Federal Government;
- **Homeland Security Advisory Councils:** Provide advice, recommendations, and expertise to the government regarding protection policy and activities.
- **Academia and Research Centers:** Provide CI/KR protection subject matter expertise, independent analysis, research and development (R&D), and educational programs.

Table S-1: Sector-Specific Agencies and HSPD-7 Assigned CI/KR Sectors

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture[1] Department of Health and Human Services[2]	Agriculture and Food
Department of Defense[3]	Defense Industrial Base
Department of Energy	Energy[4]
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Dams Emergency Services Commercial Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology Telecommunications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard[5]	Transportation Systems[6]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

[1] The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[2] The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

[3] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DOD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

[4] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[5] The U.S. Coast Guard is the SSA for the maritime transportation mode.

[6] As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

3 The CI/KR Protection Program Strategy: Managing Risk

The cornerstone of the NIPP is its risk management framework (see figure S-2) that establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk. The risk management framework is structured to promote continuous improvement to enhance CI/KR protection by focusing activities on efforts to: set security goals; identify assets, systems, networks, and functions; assess risk based on consequences, vulnerabilities and threats; establish priorities based on risk assessments; implement protective programs; and measure effectiveness. The results of these processes drive CI/KR risk-reduction and risk management activities. The framework applies to the strategic threat environment that shapes program planning, as well as to specific threats or incident situations. DHS, the SSAs, and other security partners share responsibilities for implementing the risk management framework.

DHS, in collaboration with other security partners, measures the effectiveness of CI/KR protection efforts to provide constant feedback. This allows continuous refinement of the national CI/KR protection program in a dynamic process to efficiently achieve NIPP goals and objectives.

The risk management framework is tailored and applied on an asset, system, network, or function basis, depending on the fundamental characteristics of the individual CI/KR sectors. Sectors that are primarily dependent on fixed assets and physical facilities may use a bottom-up, asset-by-asset approach, while sectors (such as Telecommunications and Information Technology) with diverse and logical assets may use a top-down business or mission continuity approach. Each sector chooses the approach that produces the most actionable results for the sector and works with DHS to ensure that the relevant risk analysis procedures are compatible with the criteria established in the NIPP.

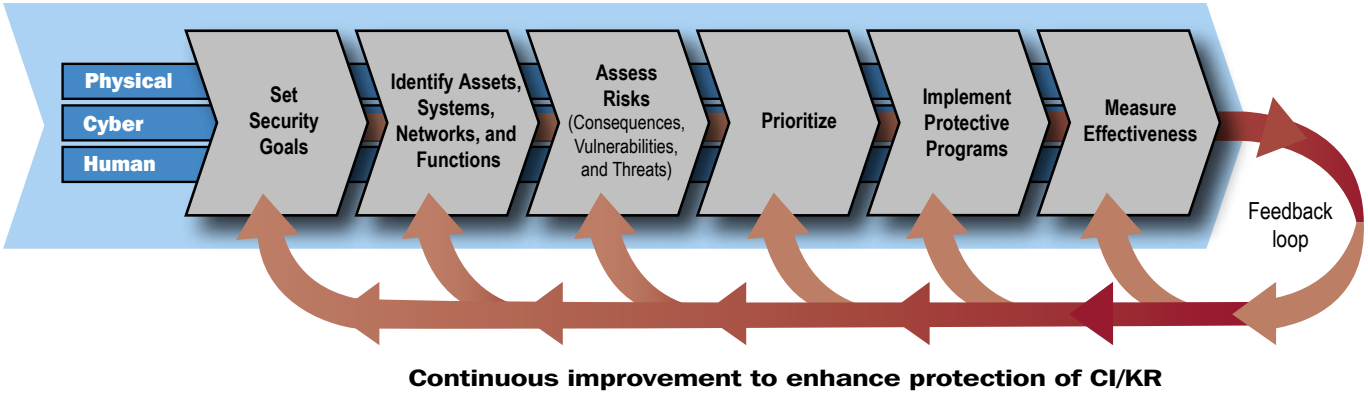
4 Organizing and Partnering for CI/KR Protection

The enormity and complexity of the Nation's CI/KR, the distributed character of its associated protective architecture, and the uncertain nature of the terrorist threat and other manmade and natural disasters make the effective implementation of protection efforts a great challenge. To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives.

The NIPP defines the organizational structures that provide the framework for coordination of CI/KR protection efforts at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through private sector and government coordinating councils that are established for each sector. Sector Coordinating Councils (SCCs) are comprised of private sector representatives. Government Coordinating Councils (GCCs) are comprised of representatives of the SSAs; other Federal departments and agencies; and State, local, and tribal governments. These councils create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing consensus approaches to CI/KR protection.

DHS also works with cross-sector entities established to promote coordination, communications, and best practices sharing across CI/KR sectors, jurisdictions, or specifically defined

Figure S-2: NIPP Risk Management Framework



geographical areas. Cross-sector issues and interdependencies are addressed among the SCCs through the Partnership for Critical Infrastructure Security (PCIS). The PCIS membership is comprised of one or more members and their alternates from each of the SCCs. Cross-sector issues and interdependencies between the GCCs will be addressed through the Government Cross-Sector Council, which is comprised of the NIPP Federal Senior Leadership Council (FSLC), and the State, Local, and Tribal Government Cross-Sector Council (SLTGCC). Additionally, DHS may convene regionally based councils to address issues that cross jurisdictions or sectors, as required.

Efficient information-sharing and information-protection processes based on mutually beneficial, trusted relationships help to ensure implementation of effective, coordinated, and integrated CI/KR protective programs and activities. Information sharing enables both government and private sector partners to assess events accurately, formulate risk assessments, and determine appropriate courses of action. The NIPP uses a network approach to information sharing that represents a fundamental change in how security partners share and protect the information needed to analyze risk and make risk-based decisions. A network approach enables secure, multidirectional information sharing between and across government and industry. The network approach provides mechanisms, using information protection protocols as required, to support the development and sharing of strategic and specific threat assessments, threat warnings, incident reports, all-hazards impact assessments, and best practices. This information-sharing approach allows security partners to assess risks, conduct risk management activities, allocate resources, and make continuous improvements to the Nation's CI/KR protective posture.

NIPP implementation relies on critical infrastructure information provided by the private sector. Much of this is sensitive business or security information that could cause serious damage to private firms, the economy, public safety, or security through unauthorized disclosure or access. The Federal Government has a statutory responsibility to safeguard CI/KR protection-related information. DHS and other Federal agencies use a number of programs and procedures, such as the Protected Critical Infrastructure Information Program, to ensure that security-related information is properly safeguarded. Other relevant programs and procedures include Sensitive Security Information for transportation activities, Unclassified Controlled Nuclear Information, contractual provisions, classified national provisions, Classified National Security Information, Law Enforcement Sensitive Information, Federal Security Information Guidelines, Federal Security Classification Guidelines, and other requirements established by law.

The CI/KR protection activities defined in the NIPP are guided by legal requirements such as those described in the Privacy Act of 1974, and are designed to achieve a balance between an appropriate level of security and protection of civil rights and liberties.

5 CI/KR Protection: An Integral Part of the Homeland Security Mission

The Homeland Security Act; other statutes and executive orders; the National Strategies for Homeland Security, for the Physical Protection of CI/KR, and for Securing Cyberspace; and a series of Homeland Security Presidential directives—most importantly HSPD-7—collectively provide the authority for the component elements outlined in the NIPP. These documents work together to provide a coordinated national approach to homeland security that is based on a common framework for CI/KR protection, preparedness, and incident management.

The NIPP defines the CI/KR protection component of the homeland security mission. Implementing CI/KR protection requires partnerships, coordination, and collaboration among all levels of government and the private sector. To enable this, the NIPP provides guidance on the structure and content of each sector's CI/KR plan, as well as the CI/KR protection-related aspects of State and local homeland security plans. This provides a baseline framework that informs the tailored development, implementation, and updating of Sector-Specific Plans; State and local homeland security strategies; and security partner CI/KR protection programs.

To be effective, the NIPP must complement other plans designed to help prevent, prepare for, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. Homeland security plans and strategies at the Federal, State, local, and tribal levels of government address CI/KR protection within their respective jurisdictions. Similarly, private sector owners and operators have responded to the post-9/11 environment by instituting a range of CI/KR protection-related plans and programs, including business continuity and resilience measures. Implementation of the NIPP will be fully coordinated between security partners to ensure that it does not result in the creation of duplicative or costly security requirements that offer little enhancement of CI/KR protection.

The NIPP and the National Response Plan (NRP) together provide a comprehensive, integrated approach to the homeland security mission. The NIPP establishes the overall risk-based approach that defines the Nation's CI/KR steady-state protective posture, while the NRP provides the approach for domestic incident management. Increases in CI/KR protective measures in the context of specific threats or that correspond to the threat conditions established in the Homeland Security Advisory System (HSAS) provide an important bridge between NIPP steady-state protection and incident management activities using the NRP.

The NRP is implemented to guide overall coordination of domestic incident management activities. NIPP partnerships and processes provide the foundation for the CI/KR dimension of the NRP, facilitating NRP threat and incident management across a spectrum of activities including incident prevention, response, restoration, and recovery.

6 Ensuring an Effective, Efficient Program Over the Long Term

To ensure an effective, efficient CI/KR protection program over the long term, the NIPP relies on the following mechanisms:

- **Building national awareness** to support the CI/KR protection program, related protection investments, and protection activities by ensuring a focused understanding of the all-hazards threat environment and of what is being done to protect and enable the timely restoration of the Nation's CI/KR in light of such threats;
- **Enabling education, training, and exercise programs** to ensure that skilled and knowledgeable professionals and experienced organizations are able to undertake NIPP-related responsibilities in the future;
- **Conducting R&D and using technology** to improve CI/KR protection-related capabilities or to lower the costs of existing capabilities so that security partners can afford to do more with limited budgets;
- **Developing, safeguarding, and maintaining data systems and simulations** to enable continuously refined risk assessment within and across sectors and to ensure preparedness for domestic incident management; and
- **Continuously improving the NIPP** and associated plans and programs through ongoing management and revision, as required.

7 Providing Resources for the CI/KR Protection Program

Chapter 7 describes an integrated, risk-based approach used to establish priorities, determine requirements, and fund the national CI/KR protection program; focus Federal grant assistance to State, local, and tribal entities; and complement relevant private sector activities. This integrated resource approach coordinates CI/KR protection programs and activities conducted by DHS, the SSAs, and other Federal entities, and focuses Federal grant funds to support national CI/KR protection efforts conducted at the State, local, and tribal levels. At the Federal level, DHS provides recommendations regarding CI/KR protection priorities and requirements to the Executive Office of the President through the National CI/KR Protection Annual Report. This report is based on information about priorities, requirements, and related program funding information that is submitted to DHS by the SSA of each sector, and assessed in the context of the National Risk Profile and national priorities. The process for allocating Federal resources through grants to State, local, and tribal governments uses a similar approach. DHS aggregates information regarding State, local, and tribal CI/KR protection priorities, requirements, and funding. DHS uses this data to inform the establishment of national priorities for CI/KR protection and to help ensure that funding is made available for protective programs that have the greatest potential for mitigating risk. This resource approach also includes mechanisms to involve private sector partners in the planning process, and supports collaboration among security partners to establish priorities, define requirements, share information, and maximize the use of finite resources.

1. Introduction

Protecting and ensuring the continuity of the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. CI/KR include the assets, systems, networks, and functions that provide vital services to the Nation. Terrorist attacks on CI/KR and other manmade or natural disasters could significantly disrupt the functioning of government and business alike, and produce cascading effects far beyond the affected CI/KR and physical location of the incident. Direct and indirect impacts could result in large-scale human casualties, property destruction, and economic disruption, and also significantly damage national morale and public confidence. Terrorist attacks using components of the Nation's CI/KR as weapons of mass destruction (WMD)[7] could have even more devastating physical, psychological, and economic consequences.

The protection of the Nation's CI/KR is essential for making America safer, more secure, and more resilient in the context of terrorist attacks and other natural and manmade hazards. Protection includes actions to mitigate the overall risk to physical, cyber, and human CI/KR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the National Infrastructure Protection Plan (NIPP), this includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident (see figure 1-1). Protection can include a wide range of activities such as improving business protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, or implementing cyber security measures, among various others. The NIPP and its complementary Sector-Specific Plans (SSPs) provide a consistent, unifying structure for integrating both existing and future CI/KR protection efforts. The NIPP also

Figure 1-1: Protection

[7] (1) Any explosive, incendiary, or poison gas (i) bomb, (ii) grenade, (iii) rocket having a propellant charge of more than 4 ounces, (iv) missile having an explosive or incendiary charge of more than one-quarter ounce, or (v) mine or (vi) similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (18 U.S.C. 2332a).

provides the core processes and mechanisms that enable all levels of government and private sector security partners to work together to implement CI/KR protection in an effective and efficient manner.

The NIPP was developed through extensive coordination with security partners at all levels of government and the private sector. NIPP processes are designed to be adapted and tailored to individual sector and security partner requirements. Participation in the implementation of the NIPP provides the government and the private sector the opportunity to use collective expertise and experience to more clearly define CI/KR protection issues and practical solutions, and to ensure that existing CI/KR protection approaches and efforts, including business continuity and resiliency planning, are recognized.

1.1 Purpose

CI/KR protection is an ongoing process with multiple intersecting elements. The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort that brings together government at all levels, the private sector, and nongovernmental organizations and international allies. The NIPP depends on supporting SSPs for full implementation of this framework throughout each CI/KR sector. SSPs are developed by the designated Federal Sector-Specific Agencies (SSAs) in close collaboration with sector security partners.

Together, the NIPP and SSPs provide the mechanisms for identifying critical assets, systems, networks, and functions; understanding threats; assessing vulnerabilities and consequences; prioritizing protection initiatives and investments based on costs and benefits so that they are applied where they offer the greatest mitigation of risk; and enhancing information-sharing mechanisms and protective measures within and across CI/KR sectors. The NIPP and SSPs will evolve in accordance with changes to the Nation's CI/KR and the threat environment, as well as evolving strategies and technologies for protecting against and responding to threats and incidents.

1.2 Scope

The NIPP considers a full range of physical, cyber, and human security elements within and across all of the Nation's CI/KR sectors. In accordance with the policy direction established in Homeland Security Presidential Directive 7 (HSPD-7), the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace, the NIPP includes an augmented focus on the protection of CI/KR from the unique and potentially catastrophic impacts of terrorist attacks. At the same time, the NIPP builds on and is structured to be consistent with and supportive of the Nation's all-hazards approach to homeland security preparedness and domestic incident management.

The NIPP addresses ongoing and future activities within each of the CI/KR sectors identified in HSPD-7 and across the sectors regionally and nationally. It defines processes and mechanisms used to prioritize protection of U.S. CI/KR (including Territories and territorial seas) and to address the interconnected global networks upon which the Nation's CI/KR depend. The processes outlined in the NIPP and the SSPs recognize that protective measures do not end at a facility's fence line or at a national border, and are often a component of a larger business continuity approach. Also considered are the implications of cross-border infrastructures, international vulnerabilities, and cross-sector dependencies and interdependencies.

1.3 Applicability

While the NIPP covers the full range of CI/KR sectors as defined in HSPD-7, it is applicable to the various public and private sector security partners in different ways. The framework generally is applicable to all security partners with CI/KR protection responsibilities and includes explicit roles and responsibilities for the Federal Government, including CI/KR under the control of independent regulatory agencies, and the legislative, executive, or judicial branches. Federal departments and agencies with specific responsibilities for CI/KR protection are required to take actions consistent with HSPD-7. The NIPP also provides an organizational structure, protection guidelines, and recommended activities for other security partners to help ensure consistent implementation of the national framework and the most effective use of resources. State,[8] local,[9] and tribal government security partners are required to establish CI/KR protection programs consistent with the National Preparedness Goal and as a condition of eligibility for certain Federal grant programs.

[8] Consistent with the definition of "State" in the Homeland Security Act of 2002, all references to States within the NIPP are applicable to Territories and include by reference any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States (Homeland Security Act).

[9] A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or, in Alaska, a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity (Homeland Security Act).

Private sector owners and operators are encouraged to participate in the NIPP partnership model and to initiate protective measures to augment existing plans for risk management, business continuity, and incident management and emergency response in line with the NIPP framework.

1.3.1 Goal

The overarching goal of the NIPP is to:

> ***Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.***

Achieving this goal requires meeting a series of objectives that include: understanding and sharing information about terrorist threats and other hazards, building security partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. Measuring progress toward achieving the NIPP goal requires that CI/KR security partners have:

- Coordinated, risk-based CI/KR plans and programs in place addressing known and potential threats and hazards;
- Structures and processes that are flexible and adaptable both to incorporate operational lessons learned and best practices and also to quickly adapt to a changing threat or incident environment;
- Processes in place to identify and address dependencies and interdependencies to allow for more timely and effective implementation of short-term protective actions and more rapid response and recovery; and
- Access to robust information-sharing networks that include relevant intelligence and threat analysis and real-time incident reporting.

1.3.2 The Value Proposition

The public-private partnership called for in the NIPP provides the foundation for effective CI/KR protection. A wide range of government and private sector partners bring core competencies that add value to the partnership. Prevention, response, mitigation, and recovery efforts are most efficient and effective when there is full participation of government and industry partners and the efforts suffer without the full participation of either partner.

The success of the partnership depends on articulating the mutual benefits to government and private sector partners. While articulating the value proposition to the government typically is clear, it is often more difficult to articulate the direct benefits of participation for the private sector. Industry provides the following capabilities, outside of government core competencies:

- Ownership and management of a vast majority of CI/KR in most sectors;
- Visibility into CI/KR assets, networks, facilities, functions, and other capabilities;
- Ability to take initial actions to respond to incidents;
- Ability to innovate and to provide products, services, and technologies to quickly focus on requirements; and
- Existing robust mechanisms useful for sharing and protecting sensitive information regarding threats, vulnerabilities, countermeasures, and best practices.

In assessing the value proposition for the private sector, there is a clear national security and homeland security interest in ensuring the collective protection of the Nation's CI/KR. Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CI/KR protection through activities such as:

- Providing owners and operators timely, analytical, accurate, and useful information on threats to CI/KR;
- Ensuring industry is engaged as early as possible in the development of initiatives and policies related to NIPP implementation and, as needed, revision of the NIPP Base Plan;
- Ensuring industry is engaged as early as possible in the development and revision of the SSPs and in planning and other CI/KR protection initiatives;
- Articulating to corporate leaders, through the use of public platforms and private communications, both the business and national security benefits of investing in security measures that exceed their business case;
- Creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted, sound security practices;
- Working with industry to develop and clearly prioritize key missions and enable their protection and/or restoration;
- Providing support for research needed to enhance future CI/KR protection efforts;

- Developing the resources to engage in cross-sector interdependency studies, through exercises, symposiums, training sessions, and computer modeling, that result in guided decision support for business continuity planning; and
- Enabling time-sensitive information sharing and restoration and recovery support to priority CI/KR facilities and services during incidents in accordance with the provisions of the Robert T. Stafford Disaster Relief and Emergency Assistance Act.

The above examples illustrate some of the ways in which the government can, by actively partnering with the private sector, add value to industry's ability to assess its own risk and refine its business continuity and security plans, as well as contribute to the security and economic vitality of the Nation. The NIPP outlines the high-level value in the overall public-private partnership for CI/KR protection. The SSPs will outline specific future activities and initiatives that articulate the corresponding value to those sector-specific CI/KR partnerships and protection activities.

1.4 Threats to the Nation's CI/KR

Presidential guidance and national strategies focus CI/KR protection efforts on addressing the emerging terrorist threat environment as an essential component of the all-hazards nature of the homeland security mission. The emergence of the terrorist threat as a reality in the 21st century presents new challenges and requires new approaches focused on intelligence-driven analyses, information sharing, and unprecedented partnerships between the government and the private sector at all levels. As a result of decades of experience responding to natural disasters, industrial accidents, and the deliberate acts of malicious individuals, the Nation's CI/KR owners and operators have adapted methods for preventing, mitigating, and responding to these incidents as a matter of business continuity. However, government and business continuity, incident, and emergency response plans and preparedness efforts must continue to adapt to a changing threat and hazard environment, and continually address vulnerabilities and gaps in CI/KR protection.

1.4.1 The Vulnerability of the U.S. Infrastructure to 21st Century Threats

America is an open, technologically sophisticated, highly interconnected, and complex Nation with a wide array of infrastructure that spans important aspects of U.S. Government, economy, and society. The majority of the CI/KR-related assets, systems, and networks are owned and operated by the private sector. In some sectors, however, such as Water and Government Facilities, the majority of owners and operators are government or quasi-governmental entities. The great diversity and redundancy of the Nation's CI/KR provide for significant physical and economic resilience in the face of terrorist attacks, natural disasters, or other emergencies, and contribute to the unprecedented strength of the Nation's economy. However, this vast and diverse aggregation of highly interconnected assets, systems, and networks may also present an attractive array of targets to terrorists and magnify greatly the potential for cascading failure in the wake of catastrophic natural or manmade disasters. Improvements in protection focusing on prioritized elements of CI/KR deemed nationally critical through implementation of the NIPP can make it more difficult for terrorists to launch attacks and lessen the impacts of any attack or other disaster that does occur.

1.4.2 The Nature of Possible Terrorist Attacks

The number and high profile of international and domestic terrorist attacks during the last decade underscore the determination and persistence of terrorist organizations. Extremist organizations have proven to be relentless, patient, opportunistic, and flexible, learning from experience and modifying tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. Current analysis of terrorist goals and motivations points to domestic and international CI/KR as potentially prime targets for terrorist attacks. As security measures around more predictable targets increase, terrorists are likely to shift their focus to less protected targets. Enhancing countermeasures to address any one terrorist tactic or target may increase the likelihood that terrorists will shift to another.

Terrorist organizations have shown an understanding of the potential consequences of carefully planned attacks on economic, transportation, and symbolic targets both within the United States and abroad. Future terrorist attacks against CI/KR across the United States could seriously threaten national security, result in mass casualties, weaken the economy, and damage public morale and confidence.

The NIPP considers a broad range of terrorist objectives, intentions, and capabilities to assess the threat to various components of the Nation's CI/KR. Based on that assessment, terrorists may contemplate attacks against the Nation's CI/KR to achieve three general types of effects:

- **Direct Infrastructure Effects:** Disruption or arrest of critical functions through direct attacks on an asset, system, or network.

- **Indirect Infrastructure Effects:** Cascading disruption and financial consequences for the government, society, and economy through public and private sector reactions to an attack. An operation could reflect an appreciation of interdependencies between different elements of CI/KR, as well as the psychological importance of demonstrating the ability to strike effectively inside the United States.
- **Exploitation of Infrastructure:** Exploitation of elements of a particular infrastructure to disrupt or destroy another target or produce cascading consequences. Attacks using CI/KR elements as a weapon to strike other targets, allowing terrorist organizations to magnify their capabilities far beyond what could be achieved using their own limited resources.

The NIPP outlines the ways in which the Department of Homeland Security (DHS) and its security partners use threat analysis to inform comprehensive risk assessments and risk-mitigation activities. The risk management framework discussed in chapter 3 strikes a balance between ways to mitigate specific and general threats. It ensures that the range of plausible attack scenarios considered is broad enough to avoid a "failure of imagination," yet contains sufficient detail to enable quantitative and qualitative risk assessment and definable actions and programs to enhance resiliency, reduce vulnerabilities, deter threats, and mitigate potential consequences.

1.5 All-Hazards and CI/KR Protection

In addition to addressing CI/KR protection related to terrorist threats, the NIPP also describes activities relevant to CI/KR protection and preparedness in an all-hazards context. The direct impacts, disruptions, and cascading effects of natural disasters (e.g., Hurricanes Katrina and Rita, the Northridge earthquake, etc.) and manmade incidents (e.g., the Three Mile Island Nuclear Power Plant accident or the Exxon Valdez oil spill) on the Nation's CI/KR are well documented. The recent experience in the wake of Hurricane Katrina, for example, underscored the vulnerabilities and interdependencies of the Nation's CI/KR.

Many owners and operators, government emergency managers, and first-responders have developed strategies, plans, policies, and procedures to prepare for, mitigate, respond to, and recover from a variety of natural and manmade incidents. The NIPP framework recognizes these efforts and provides an augmented focus on the protection of America's CI/KR against terrorist attacks. In fact, the day-to-day public-private coordination structures, information-sharing network, and risk management framework used to implement NIPP steady-state CI/KR protection efforts continue to function and provide the CI/KR protection dimension for incident management activities under the National Response Plan (NRP). The NIPP, and the public and private sector partnership that it represents, works in conjunction with other plans and initiatives to provide a stronger foundation for preparedness in an all-hazards context. NIPP elements include:

- A comprehensive approach that integrates authorities, capabilities, and resources on a national, regional, and local scale;
- A complete and accurate assessment of the Nation's CI/KR that not only helps inform the prioritization of protection activities, but also enables response and recovery efforts;
- An organization and coordinating structure to enable effective partnership between and among Federal, State, local, and tribal governments, regional and international entities, as well as the private sector;
- An integrated approach to enhancing protection of the physical, cyber, and human elements of the Nation's CI/KR in which individual security measures complement one another; and
- The development and use of sophisticated analytical and modeling tools to help inform effective risk-mitigation programs in an all-hazards context.

1.6 Planning Assumptions

The NIPP is based on the following planning assumptions that relate to the sector-specific and cross-sector nature of the CI/KR protection mission, the adaptive nature of the terrorist threat, and the most effective approaches to all-hazards CI/KR protection.

1.6.1 Sector-Specific Nature of CI/KR Protection

- Approaches to CI/KR protection and risk management vary based on sector business characteristics, risk landscape, protection authorities, requirements, and maturity;
- Assets, systems, and networks vary in criticality within and across CI/KR sectors;
- Successful CI/KR protection requires robust baseline information on assets, systems, networks, and functions within and across CI/KR sectors, regions,[10] and specific localities;
- Owners and operators conduct risk management planning and invest in security from a business perspective and may

[10] Areas with shared geography, economies, or other characteristics that can serve as the focal points for CI/KR protection through public and private partnerships.

look for various types of incentives to elicit maximum participation in CI/KR protection;

- In some sectors, private firms own the vast majority of CI/KR;
- Some regulatory agencies may already impose protective measure requirements on private sector owners and operators. Coordination between the private sector, DHS, and the SSAs is required to address measures for threats beyond the regulatory baseline; and
- Strong relationships among security partners are essential to meet the overarching goal and supporting objectives set forth in the NIPP.

1.6.2 Cross-Sector Dependencies and Interdependencies

- In some cases, a failure in one sector may significantly impact another sector's ability to perform necessary and critical functions; and
- Many CI/KR sectors rely on the service grids of the Energy, Information Technology, Telecommunications, and Transportation sectors. Failures in these sectors can prevent others from functioning properly. Relevant sector dependencies and interdependencies must be considered when developing SSPs.

1.6.3 Adaptive Nature of the Terrorist Threat

- CI/KR protection activities take place in a highly dynamic threat environment. The general threat environment changes as the capabilities and the intentions of terrorists evolve;
- It is not practical or feasible to protect all assets, systems, and networks against every possible terrorist attack vector. A risk-based approach enhanced by intelligence and information analysis and reporting provides the basis for an effective risk management strategy and efficient resource allocation;
- CI/KR protection planning at the national and sector levels must address the full range of plausible threats and hazards, not just those most frequently reported or considered to be the most likely to occur; and
- A proactive approach is required to enhance decision-making processes, provide advance warning to potentially targeted or vulnerable CI/KR, and assist owners and operators in taking protective steps to enhance CI/KR protection in an all-hazards context.

1.6.4 All-Hazards Nature of CI/KR Protection

- Natural disasters such as floods, hurricanes, tornadoes, wildfires, pandemics, and earthquakes, and unintentional manmade disasters such as oil spills or radiological accidents, also pose a threat to the Nation's CI/KR; and
- Efforts to enhance the protection of CI/KR from terrorist attacks should support all-hazards preparedness and response whenever possible.

1.7 Special Considerations

CI/KR protection planning involves special consideration for protection of sensitive infrastructure information, the unique cyber and human elements of infrastructure, and complex international relationships.

Assets, systems, and networks include one or more of the following elements:

Physical—tangible property;

Cyber—electronic information and communications systems, and the information contained therein; and

Human—critical knowledge of functions or people uniquely susceptible to attack.

1.7.1 Protection of Sensitive Information

Protection of sensitive information involves:

- **Protection** from unauthorized access and public disclosure;
- **Security** to guard against damage, theft, modification, or exploitation (e.g., firewalls, physical security); and
- **Detection** to identify malicious activity affecting an electronic information or communications system.

- Partnership with the private sector requires the establishment of mutually beneficial, trusted relationships supported by a network approach to providing access to information and a business continuity approach to minimizing or managing risk;
- Great care must be taken by the government to ensure that sensitive infrastructure information is protected and used appropriately to enhance the protection of the Nation's CI/KR;

- Information on specific industry assets and vulnerabilities is particularly sensitive because public release may lead to breaches in security, competitive advantage, and/or adverse impacts on an industry's position in the marketplace; and
- DHS does not have broad regulatory authority over CI/KR and cannot compel private sector entities to submit infrastructure or operational information. Rather, DHS works in partnership with industry and the SSAs to identify the necessary information and promote the trusted exchange of such data.

1.7.2 The Cyber Dimension

Cyber infrastructure includes electronic information and communications systems, and the information contained in those systems. Computer systems, control systems such as Supervisory Control and Data Acquisition (SCADA) systems, and networks such as the Internet are all part of cyber infrastructure.

Information and communications systems are composed of hardware and software that process, store, and communicate. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information.

- The U.S. economy and national security are highly dependent upon the global cyber infrastructure. Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of CI/KR;
- A spectrum of malicious actors could conduct attacks against the cyber infrastructure using cyber attack tools. Because of the interconnected nature of the cyber infrastructure, these attacks could spread quickly and have a debilitating impact;
- The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation's risk to cyber threats if cyber security is not addressed and integrated appropriately;
- The interconnected and interdependent nature of the Nation's CI/KR makes it problematic to address the protection of physical and cyber assets independently;
- Cyber security includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Cyber security also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster; and
- The NIPP addresses reducing cyber risk and enhancing cyber security in two ways: (1) as a cross-sector cyber element that involves DHS, SSAs, and private sector owners and operators; and (2) as a major component of the Information Technology sector's responsibility in partnership with the Telecommunications sector.

1.7.3 The Human Element

- The NIPP recognizes that each CI/KR asset, system, and network is made up of physical and cyber components, and human elements;
- The human element requires:
  - Identifying and preventing the insider threat resulting from infiltration or individual employees determined to do harm;
  - Identifying, protecting, and supporting (e.g., via cross-training) employees and other persons with critical knowledge or functions; and
  - Identifying and mitigating fear tactics used by terrorist agents and disaffected insiders;
- Assessing human element vulnerabilities is more subjective than assessing the physical or cyber vulnerabilities of corresponding assets, systems, and networks; and
- Diverse protective programs and actions to address threats posed by employees and to employees need to be put into place across all sectors.

1.7.4 International CI/KR Protection

- The NIPP addresses international CI/KR protection, including interdependencies and vulnerabilities based on threats that originate outside the country or transit through it;
- The Federal Government and the private sector work with foreign governments and international/multinational organizations to enhance the confidentiality, integrity, and availability of cyber infrastructure and products;

- Protection of assets, systems, and networks that operate across or near the borders with Canada and Mexico, or rely on other international aspects to enable critical functionality, requires coordination with, and planning and/or sharing resources among, neighboring governments at all levels, as well as private sector CI/KR owners and operators;
- The Federal Government and private sector corporations have a significant number of facilities located outside the United States that may be considered CI/KR;
- Special consideration is required when CI/KR is extensively integrated into an international or global market (e.g., financial services, agriculture, energy, transportation, telecommunications, or information technology) or when a sector relies on inputs that are not within the control of U.S. entities; and
- Special consideration is required when government facilities and functions are directly affected by foreign-owned and -operated commercial facilities.

1.8 Achieving the Goal of the NIPP

Achieving the NIPP goal of building a safer, more secure, and more resilient America requires actions that address the following principal objectives:

- Understanding and sharing information about terrorist threats and other hazards;
- Building security partnerships to share information and implement CI/KR protection programs;
- Implementing a long-term risk management program that includes:
  - Hardening and ensuring the resiliency of CI/KR against known threats and hazards, as well as other potential contingencies;
  - Processes to interdict human threats to prevent potential attacks;
  - Planning for rapid response to CI/KR disruptions to limit the impacts on public health and safety, the economy, and government functions; and
  - Planning for rapid CI/KR restoration and recovery for those events that are not preventable; and
- Maximizing efficient use of resources for CI/KR protection.

This section provides a summary of the actions needed to address these objectives. More detailed discussions of these actions are included in the chapters that follow.

1.8.1 Understanding and Sharing Information

One of the essential elements needed to achieve the Nation's CI/KR protection goals is to ensure the availability and flow of accurate, timely, and relevant information and/or intelligence about terrorist threats and other hazards, information analysis, and incident reporting. This includes actions to:

- Establish effective information-sharing processes and protocols among security partners;
- Provide intelligence and information to SSAs and other CI/KR sector partners as permitted by law;
- Analyze, warehouse, and share risk assessment data in a secure manner consistent with relevant legal requirements and information protection responsibilities;
- Provide protocols for real-time threat and incident reporting, alert, and warning; and
- Provide protocols for the protection of sensitive information.

Chapter 3 details the threat analysis process and products aimed at better understanding and characterizing terrorist threats. Chapter 4 describes the NIPP network approach to information sharing and the process for protecting sensitive CI/KR-related information.

1.8.2 Building Security Partnerships

Building security partnerships represents the foundation of the national CI/KR protection effort. These partnerships provide a framework to:

- Exchange ideas, approaches, and best practices;
- Facilitate security planning and resource allocation;
- Establish effective coordinating structures among security partners;
- Enhance coordination with the international community; and
- Build public awareness.

Chapters 2 and 4 detail security partner roles and responsibilities related to CI/KR protection, as well as specific mechanisms for governance, coordination, and information sharing necessary to enable effective partnerships.

1.8.3 Implementing a Long-Term CI/KR Risk Management Program

The long-term risk management program detailed in the NIPP includes processes to:

- Establish a risk management framework to guide CI/KR protection programs and activities;
- Identify and regularly update the status of CI/KR protection programs within and across sectors;
- Conduct and update risk assessments at the asset, system, network, sector, cross-sector, regional, national, and international levels;
- Develop and deploy new technologies to enable more effective and efficient CI/KR protection; and
- Provide a system for continuous measurement and improvement of CI/KR protection, including:
  - Establishing performance metrics to assess the effectiveness of protective programs; and
  - Updating the NIPP and SSPs as required.

The NIPP also specifies the processes, key initiatives, and milestones necessary to implement an effective long-term CI/KR risk management program. Chapter 3 provides details regarding the NIPP risk management framework; chapter 6 addresses issues important for sustaining and improving CI/KR protection over the long term.

1.8.4 Maximizing Efficient Use of Resources for CI/KR Protection

Maximizing the efficient use of resources for CI/KR protection includes a coordinated and integrated annual process for program implementation that:

- Supports prioritization of programs and activities within and across sectors;
- Informs the annual Federal process regarding planning, programming, and budgeting for national-level CI/KR protection;
- Helps to align the resources of the Federal budget to the CI/KR protection mission and goals, and to enable tracking and accountability for the expenditure of public funds;
- Takes into account State, local, and tribal government and private sector considerations related to planning, programming, and budgeting;
- Draws on expertise across organizational and national boundaries;
- Shares expertise and speeds implementation of best practices;
- Recognizes the need to build a business case based on the NIPP value proposition for further private sector CI/KR protection investments; and
- Identifies potential incentives for security-related activities where they do not naturally exist in the marketplace.

Chapter 5 explains how a coordinated national approach to the CI/KR protection mission enables the efficient use of resources. Efficient use of resources requires a deliberate process to continuously improve the technology, databases, data systems, and other approaches used to protect CI/KR and manage risk. These processes are detailed in chapter 6. Chapter 7 describes the annual processes required to establish investment mechanisms for CI/KR protection that reflect appropriate coordination with SSAs and other security partners regarding resource prioritization and allocation. Also discussed are processes to utilize grants and other funding authorities to maximize and focus the use of resources to support program priorities.

More information about the NIPP is available on the Internet at: **www.dhs.gov/nipp** or by contacting DHS at: **nipp@dhs.gov**

2. Authorities, Roles, and Responsibilities

Improving the protection of the Nation's CI/KR in an all-hazards environment requires a comprehensive, unifying organization; clearly defined roles and responsibilities; and close cooperation across all levels of government and the private sector. Protection authorities, requirements, resources, capacities, and risk landscapes vary widely across governmental jurisdictions, sectors, and individual industries and enterprises. This reality presents a complex set of challenges in terms of NIPP compliance and performance measurement. Hence, successful implementation of the NIPP and supporting SSPs depends on an effective partnership framework that fosters integrated, collaborative engagement and interaction; establishes a clear division of responsibilities among diverse Federal, State, local, tribal, and private sector security partners; and efficiently allocates the Nation's protection resources based on risk and need.

This chapter includes a brief overview of the relevant authorities and outlines the principal roles and responsibilities of DHS; SSAs; other Federal departments and agencies; State, local, and tribal jurisdictions; private sector owners and operators; and other security partners who share responsibility in protecting the Nation's CI/KR under the NIPP. A comprehensive and unequivocal understanding of these roles and responsibilities provides the foundation for an effective and sustainable national CI/KR protection effort.

2.1 Authorities

The roles and responsibilities described in this chapter are derived from a series of authorities, including the Homeland Security Act of 2002, other CI/KR protection-related legislation, executive orders, Homeland Security Presidential directives, and Presidential strategies. The National Strategy for Homeland Security established the national CI/KR vision with a charge to "forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructures and key assets from terrorist attack."[11] HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, provided the direction to implement this vision. More detailed information on these and other CI/KR protection-related authorities is included in appendix 2A.

The Homeland Security Act provides the primary authority for the overall homeland security mission and outlines DHS responsibilities in the protection of the Nation's CI/KR. It established the DHS mission, including "reducing the Nation's vulnerability to terrorist attacks," major disasters, and other emergencies, and charged the department with the responsibility for evaluating vulnerabilities and ensuring that steps are implemented to protect the high-risk elements of America's CI/KR, including food and water systems, agriculture, health systems and emergency services, information technology, telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, and dams), transportation (air, highways, rail, ports, and waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons. Title II, section 201, of

[11] The National Strategy for Homeland Security uses the term "key assets," defined as individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage the Nation's morale or confidence. The Homeland Security Act and HSPD-7 use the term "key resources," defined more generally to capture publicly or privately controlled resources essential to the minimal operations of the economy or government. "Key resources" is the current terminology.

the act assigned primary responsibility to DHS to develop a comprehensive national plan for securing CI/KR and for recommending "the measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities."

A number of other statutes provide authorities both for cross-sector and sector-specific CI/KR protection efforts. Some examples of other CI/KR protection-related legislation include: The Public Health Security and Bioterrorism Preparedness and Response Act of 2002, which was intended to improve the ability of the United States to prevent, prepare for, and respond to acts of bioterrorism and other public health emergencies; the Maritime Transportation Security Act; the Energy Policy and Conservation Act; the Critical Infrastructure Information Act; the Federal Information Security Management Act; and various others.

These separate authorities are tied together as part of the national approach for CI/KR protection through the unifying framework established in HSPD-7. HSPD-7, issued in December 2003, established the U.S. policy for "enhancing protection of the Nation's CI/KR." HSPD-7 establishes a framework for security partners to identify, prioritize, and protect the Nation's CI/KR from terrorist attacks, with an emphasis on protecting against catastrophic health effects and mass casualties. The directive sets forth the roles and responsibilities for DHS; SSAs; other Federal departments and agencies; State, local, and tribal governments; the private sector; and other security partners. The following sections address security partner roles and responsibilities under this integrated approach.

2.2 Roles and Responsibilities

Given the fact that terrorist attacks and certain natural or manmade disasters can have national-level impact, it is incumbent upon the Federal Government to provide overarching leadership and coordination in the CI/KR protection mission area.

2.2.1 Department of Homeland Security

Under HSPD-7, DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance CI/KR protection, including collaborative development of the NIPP and supporting SSPs; developing and implementing comprehensive, multi-tiered risk management programs and methodologies; developing cross-sector and cross-jurisdictional protection guidance, guidelines, and protocols; and recommending risk management and performance criteria and metrics within and across sectors. Per HSPD-7, DHS is also a focal point for the security of cyberspace. HSPD-7 establishes a central source for coordinating uniform security practices and harmonizing security programs across and within government agencies. In the directive, the President designates the Secretary of Homeland Security as the "principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources." The Secretary of Homeland Security is responsible for addressing the complexities of the Nation's Federal system of government and its multifaceted and interdependent economy, as well as for establishing structures to enhance the close cooperation between the private sector and government at all levels to initiate and sustain an effective CI/KR protection program.

In addition to these overarching leadership and cross-sector responsibilities, DHS serves as the SSA for 10 of the CI/KR sectors identified in HSPD-7: Information Technology; Telecommunications; Transportation; Chemical; Emergency Services; Commercial Nuclear Reactors, Material, and Waste; Postal and Shipping; Dams; Government Facilities; and Commercial Facilities. Specific SSA responsibilities are discussed in section 2.2.2.

Additional DHS CI/KR protection roles and responsibilities include:

- Identifying, prioritizing, and coordinating Federal action in support of the protection of nationally critical assets, systems, and networks, with a particular focus on CI/KR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a WMD;
- Coordinating, facilitating, and supporting the overall process for building security partnerships and leveraging sector-specific security expertise, relationships, and resources across CI/KR sectors, including oversight and support of the sector partnership model described in chapter 4; cooperation with Federal, State, local, and tribal security partners; and collaborating with the Department of State to reach out to foreign countries and international organizations to strengthen the protection of U.S. CI/KR;
- Establishing and maintaining a comprehensive, multi-tiered, dynamic information-sharing network designed to provide timely and actionable threat information, assessments, and warnings to public and private sector security

partners. This responsibility includes protecting sensitive information voluntarily provided by the private sector and facilitating the development of sector-specific and cross-sector information-sharing and analysis systems, mechanisms, and processes;

- Coordinating national efforts for the security of cyber infrastructure, including precursors and indicators of an attack, and understanding those threats in terms of CI/KR vulnerabilities;
- Coordinating, facilitating, and supporting comprehensive risk assessment programs for high-risk CI/KR, identifying protection priorities across sectors and jurisdictions, and integrating CI/KR protective programs with the all-hazards approach to domestic incident management described in HSPD-5;
- Facilitating the sharing of CI/KR protection best practices and processes, and risk assessment methodologies and tools across sectors and jurisdictions;
- Sponsoring CI/KR protection-related research and development (R&D), demonstration projects, and pilot programs;
- Seeding development and transfer of advanced technologies while leveraging private sector expertise and competencies, including participation in the development of voluntary consensus standards or best practices as appropriate;
- Promoting national-level CI/KR protection education, training, and awareness in cooperation with State, local, tribal, and private sector partners;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the Homeland Security Advisory System (HSAS);
- Providing real-time (24/7) threat and incident reporting;
- Conducting modeling and simulations to analyze sector, cross-sector, and regional dependencies and interdependencies, to include cyber, and sharing the results with security partners, as appropriate;
- Informing the annual Federal budget process based on CI/KR risk and need in coordination with SSAs and other security partners;
- Monitoring performance measures for the national CI/KR protection program and NIPP implementation process to enable continuous improvement, and providing annual CI/KR protection reports to the Executive Office of the President that include current status, priorities, progress, and gaps in program authorities or resources, and recommended corrective actions;
- Integrating national efforts for the protection and recovery of critical information systems and cyber components of physical CI/KR, including analysis, warning, information-sharing, vulnerability reduction, and mitigation activities and programs;
- Evaluating preparedness for CI/KR protection across sectors and jurisdictions as a component of the National Exercise Program;
- Documenting lessons learned from exercises, actual incidents, and pre-disaster mitigation efforts, and applying those lessons, where applicable, to CI/KR protection efforts;
- Working with the Department of State, SSAs, and other security partners to ensure that U.S. CI/KR protection efforts are fully coordinated with international partners; and
- Evaluating the need for and coordinating the protection of additional CI/KR categories over time, as appropriate.

2.2.2 Sector-Specific Agencies

Recognizing that each CI/KR sector possesses its own unique characteristics, operating models, and risk landscape, HSPD-7 designates Federal Government SSAs for each of the CI/KR sectors (see table 2-1). SSAs are responsible for working with DHS to implement the NIPP sector partnership model and risk management framework, develop protective programs and related requirements, and provide sector-level CI/KR protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7. Working in collaboration with security partners, they are responsible for developing and submitting SSPs and sector-level performance feedback to DHS to enable national cross-sector CI/KR protection program gap assessments.

In accordance with HSPD-7, SSAs are also responsible for collaborating with private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms within the sector. This includes supporting sector coordinating mechanisms to facilitate sharing of information on physical and cyber threats, vulnerabilities, incidents, recommended protective measures, and security-related best practices. This also includes encouraging voluntary security-related information sharing, where possible, among private entities within the sector, as well as among public and private entities.

Table 2-1: Sector-Specific Agencies and HSPD-7 Assigned CI/KR Sectors

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture[12] Department of Health and Human Services[13]	Agriculture and Food
Department of Defense[14]	Defense Industrial Base
Department of Energy	Energy[15]
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Dams Emergency Services Commercial Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Telecommunications	Information Technology Telecommunications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard[16]	Transportation Systems[17]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

[12] The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[13] The Department of Health and Human Services (HHS) is responsible for food other than meat, poultry, and egg products.

[14] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DOD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

[15] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[16] The U.S. Coast Guard (USCG) is the SSA for the maritime transportation mode.

[17] As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

SSAs perform the activities above, as appropriate and consistent with existing authorities (including regulatory authorities in some instances), in close cooperation with other security partners. HSPD-7 requires SSAs to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors. Consistent with this requirement, DHS will provide reporting guidance and templates that include requests for specific information, such as sector CI/KR protection priorities, requirements, and resources. SSAs also are responsible for outlining these sector-specific CI/KR protection requirements and related budget projections as a component of their annual budget submissions to the Office of Management and Budget (OMB).

Additional SSA responsibilities include:

- Identifying, prioritizing, and coordinating the protection of sector-level CI/KR with a particular focus on CI/KR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a WMD;
- Managing the overall process for building security partnerships and leveraging CI/KR security expertise, relationships, and resources within the sector, including sector-level oversight and support of the sector partnership model described in chapter 4;
- Coordinating, facilitating, and supporting comprehensive risk assessment/management programs for high-risk CI/KR, identifying protection priorities, and incorporating CI/KR protection activities as a key component of the all-hazards approach to domestic incident management within the sector;
- Facilitating the sharing of real-time incident notification, as well as CI/KR protection best practices and processes, and risk assessment methodologies and tools within the sector;
- Promoting sector-level CI/KR protection education, training, and awareness in coordination with State, local, tribal, and private sector partners;
- Informing the annual Federal budget process based on CI/KR risk and protection needs in coordination with security partners and allocating resources for CI/KR protection accordingly;
- Monitoring performance measures for sector-level CI/KR protection and NIPP implementation activities to enable continuous improvement, and reporting progress and gaps to DHS;
- Contributing to the annual National Critical Infrastructure Protection Research and Development (NCIP R&D) Plan;
- Identifying/recommending appropriate strategies to encourage private sector participation;
- Supporting DHS-initiated data calls to populate the National Asset Database (NADB), enable national-level risk assessment, and inform national-level resource allocation;
- Supporting protocols for the Protected Critical Infrastructure Information (PCII) Program;
- Working with DHS to develop, evaluate, validate, or modify sector-specific risk assessment tools;
- Supporting sector-level dependency, interdependency, consequence, and other analysis as required;
- Coordinating sector-level participation in the National Exercise Program, Homeland Security Exercise and Evaluation Program (HSEEP), and other sector-level activities;
- Assisting sector security partners in their efforts to:
  - Organize and conduct protection and continuity-of-operations planning, and elevate awareness and understanding of threats and vulnerabilities to their assets, systems, and networks; and
  - Identify and promote effective sector-specific CI/KR protection practices and methodologies;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the HSAS;
- Understanding and mitigating sector-specific cyber risk by developing or encouraging appropriate protective measures, information-sharing mechanisms, and emergency recovery plans for cyber assets, systems, and networks within the sector and interdependent sectors; and
- Supporting DHS and Department of State efforts to integrate U.S. CI/KR protection programs into the international and global markets, and address relevant dependency, interdependency, and cross-border issues.

2.2.3 Other Federal Departments, Agencies, and Offices

All Federal departments and agencies function as security partners in coordination with DHS and the SSAs. In accordance with HSPD-7, they are required to cooperate with DHS in implementing CI/KR protection efforts, consistent with the Homeland Security Act and other applicable legal authorities. In this capacity, they support implementation of the NIPP and SSPs, as appropriate, and are responsible for identification, prioritization, assessment, remediation, and enhancing the protection of CI/KR under their control. HSPD-7 also requires that all departments and agencies work with the sectors relevant to their responsibilities to reduce the consequences of catastrophic failures not caused by acts of terrorism.

Federal departments and agencies that are not designated as SSAs, but have unique responsibilities, functions, or expertise in a particular CI/KR sector will:

- Assist in assessing risk, prioritizing CI/KR, and enabling protective actions and programs within that sector;
- Support the national goal of enhancing CI/KR protection through their roles as the regulatory agencies for owners and operators represented within specific sectors when so designated by statute; and
- Collaborate with all relevant security partners to share security-related information within the sector, as appropriate.

Depending on their regulatory roles and their relationships with the SSAs, these agencies may play a supporting role in developing and implementing SSPs and related protective activities within the sector.

Under HSPD-7, a number of Federal departments and agencies and components of the Executive Office of the President have special functions related to CI/KR protection. The following section addresses Federal departments, agencies, and commissions specifically identified in HSPD-7. Many other Federal entities have sector-specific or cross-sector authorities and responsibilities that are more appropriately addressed in the SSPs.

- **The Department of State**, in coordination with DHS and the Departments of Justice (DOJ), Commerce, Defense, and Treasury, works with foreign governments and international organizations to strengthen U.S. CI/KR protection efforts.
- **The Department of Justice**, including the Federal Bureau of Investigation (FBI), acts to reduce terrorist threats, and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of CI/KR in collaboration with DHS.
- **The Department of Commerce** works with DHS, the private sector, and research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act to ensure the timely availability of industrial products, materials, and services to meet homeland security requirements, and to address economic security issues.
- **The Department of Transportation** (DOT) collaborates with DHS on all matters related to transportation security and transportation infrastructure protection, and is additionally responsible for operating the National Airspace System. DOT and DHS collaborate on regulating the transportation of hazardous materials by all modes (including pipelines).
- **The Nuclear Regulatory Commission** (NRC) works with DHS and the Department of Energy (DOE), as appropriate, to ensure the protection of commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste. In addition, the NRC collaborates with DHS on any changes in the protective measures for this sector.
- **The Intelligence Community, the Department of Defense, and other appropriate Federal departments**, such as the Department of the Interior and DOT, are collaborating with DHS on the development and implementation of a geospatial program to map, image, analyze, and sort CI/KR data using commercial satellite and airborne systems, as well as associated agency capabilities. DHS works with these Federal departments and agencies to identify and help protect those positioning, navigation, and timing services, such as global positioning systems (GPS), that are critical enablers for CI/KR sectors such as Banking and Finance and Telecommunications. DHS and the intelligence community also collaborate with other agencies, such as the Environmental Protection Agency, that manage data addressed by geographic information systems.

- **The Homeland Security Council** ensures the coordination of interagency policy related to physical and cyber CI/KR protection based on advice from the Critical Infrastructure Protection Policy Coordinating Committee (PCC). This PCC is chaired by a Federal officer or employee designated by the Assistant to the President for Homeland Security.
- **The Office of Science and Technology Policy** coordinates with DHS to further interagency R&D related to CI/KR protection.
- **The Office of Management and Budget** oversees the implementation of government-wide policies, principles, standards, and guidelines for Federal Government computer security programs.

2.2.4 State, Local, and Tribal Governments

State, local, and tribal governments are responsible for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities and industries within their jurisdictions. They also play a very important and direct role in enabling the protection of the Nation's CI/KR, including CI/KR under their control, as well as CI/KR owned and operated by other NIPP security partners within their jurisdictions. The efforts of these public entities are critical to the effective implementation of the NIPP, SSPs, and various jurisdictionally focused protection plans. They are equally critical in terms of enabling time-sensitive, post-event CI/KR response, restoration, and recovery activities.

Security partners at all levels of government have recently developed homeland security strategies that align with and support the priorities established in the National Preparedness Goal. With the inclusion of NIPP implementation as one of these national priorities, CI/KR protection programs form an essential component of State, local, and tribal homeland security strategies, particularly with regard to establishing funding priorities and informing security investment decisions. To permit effective NIPP implementation and performance measurement at each jurisdictional level, these protection programs should reference all core elements of the NIPP framework, including key cross-jurisdictional security and information-sharing linkages, as well as specific CI/KR protective programs focused on risk management. These programs play a primary role in the identification and protection of CI/KR locally and also support DHS and SSA efforts to identify, ensure connectivity with, and enable the protection of CI/KR of national-level criticality within the jurisdiction.

2.2.4.1 State and Territorial Governments

State governments are responsible for establishing security partnerships, facilitating coordinated information sharing, and enabling planning and preparedness for CI/KR protection within their jurisdictions. They serve as crucial coordination hubs, bringing together prevention, protection, response, and recovery authorities; capacities; and resources among local jurisdictions, across sectors, and between regional entities. States also act as conduits for requests for Federal assistance when the threat or incident situation exceeds the capabilities of public and private sector security partners at lower jurisdictional levels. States receive CI/KR information from the Federal Government to support the national and State CI/KR protection programs.

State governments are responsible for developing and implementing statewide/regional CI/KR protection programs that reflect the full range of NIPP-related activities. State programs should address all relevant aspects of CI/KR protection, leverage support from homeland security assistance programs that apply across the homeland security mission area, and reflect priority activities in their strategies to ensure that resources are effectively allocated. Effective statewide and regional CI/KR protection efforts should be integrated into the overarching homeland security program framework at the State level to ensure that prevention, protection, response, and recovery efforts are synchronized and mutually supportive. CI/KR protection at the State level must cut across all sectors present within the State and support national, State, and local priorities. The program also should explicitly address unique geographical issues, including trans-border concerns, as well as interdependencies among sectors and jurisdictions within those geographical boundaries.

Specific CI/KR protection-related activities include:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local jurisdictions and regional partners;
- Developing a unified approach to CI/KR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant stakeholders within their jurisdictions;
- Identifying, implementing, and monitoring a risk management plan and taking corrective actions as appropriate;

- Participating in significant national, regional, and local awareness programs to encourage appropriate management and security of cyber systems;
- Acting as conduits for requests for Federal assistance when the threat or current situation exceeds the capabilities of State and local jurisdictions and private entities resident within them;
- Facilitating the exchange of security information, including threat assessments, attack indications and warnings, and advisories, within and across jurisdictions and sectors therein;
- Participating in the NIPP sector partnership model, including Government Coordinating Councils (GCCs), Sector Coordinating Councils (SCCs), and other CI/KR governance efforts and SSP planning efforts relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CI/KR protection mission in accordance with relevant plans and strategies;
- Sharing information on CI/KR deemed critical from national, State, regional, local, and/or tribal perspectives to enable prioritized protection and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Addressing unique geographical issues, including trans-border concerns, dependencies, and interdependencies among the sectors within the jurisdiction;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the HSAS;
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CI/KR protection context;
- Identifying and communicating requirements for CI/KR-related R&D to DHS; and
- Providing information, as part of the grants process and/or homeland security strategy updates, regarding State priorities, requirements, and CI/KR-related funding projections.

2.2.4.2 Local Governments

Local governments represent the front lines for homeland security and, more specifically, for CI/KR protection and implementation of the NIPP partnership model. They provide critical public services and functions in conjunction with private sector owners and operators. In some sectors, local government entities own and operate CI/KR such as water, stormwater, and electric utilities. Most disruptions or malevolent acts that impact CI/KR begin and end as local situations. Local authorities typically shoulder the weight of initial prevention, response, and recovery operations until coordinated support from other sources becomes available, regardless of who owns or operates the affected asset, system, or network. As a result, local governments are critical partners under the NIPP framework. They drive emergency preparedness, as well as local participation in NIPP and SSP implementation across a variety of jurisdictional security partners, including government agencies, owners and operators, and private citizens in the communities they serve.

CI/KR protection focus at the local level should include, but is not limited to:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local agencies, businesses, and citizens;
- Developing a unified approach at the local level to CI/KR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant security partners within the jurisdiction;
- Identifying, implementing, and monitoring a risk management plan, and taking corrective actions as appropriate;
- Participating in significant national, regional, and local awareness programs to encourage appropriate management and security of cyber systems;
- Facilitating the exchange of security information, including threat assessments, attack indications and warnings, and advisories, among security partners within the jurisdiction;
- Participating in the NIPP sector partnership model, including GCCs, SCCs, and other CI/KR governance efforts and SSP planning efforts relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve

the CI/KR protection mission in accordance with relevant plans and strategies;

- Sharing information with security partners, as appropriate, on CI/KR deemed critical from the local perspective to enable prioritized protection and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Addressing unique geographical issues, including trans-border concerns, dependencies, and interdependencies among agencies and enterprises within the jurisdiction;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the HSAS;
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CI/KR protection context; and
- Conducting CI/KR protection public awareness activities.

2.2.4.3 Tribal Governments

Tribal government roles and responsibilities regarding CI/KR protection generally mirror those of State and local governments as detailed above. Tribal governments are accountable for the public health, welfare, and safety of tribal members, as well as the protection of CI/KR and continuity of essential services under their jurisdiction. Under the NIPP partnership model, tribal governments must ensure close coordination with Federal, State, local, and international counterparts to achieve synergy in the implementation of the NIPP and SSP frameworks within their jurisdictions. This is particularly important in the context of information sharing, risk analysis and management, awareness, preparedness planning, protective program investments and initiatives, and resource allocation. To facilitate this interaction, tribal governments, as appropriate, should be active participants in the NIPP governance structures detailed in chapter 4.

2.2.4.4 Regional Partners

Regional security partnerships include a variety of public-private sector initiatives that cross jurisdictional and/or sector boundaries and focus on homeland security preparedness, protection, response, and recovery within or serving the population of a defined geographical area. Specific regional initiatives range in scope from organizations that include multiple jurisdictions and industry partners within a single State to groups that involve jurisdictions and enterprises in more than one State and across international borders. In many cases, State governments also collaborate through the adoption of interstate compacts to formalize regionally based partnerships regarding CI/KR protection.

Security partners leading or participating in regional initiatives are encouraged to capitalize on the larger area- and sector-specific expertise and relationships to:

- Promote collaboration among security partners in implementing NIPP-related CI/KR risk assessment and protection activities;
- Facilitate education and awareness of CI/KR protection efforts occurring within their geographical areas;
- Coordinate regional exercise and training programs, including a focus on CI/KR protection collaboration across jurisdictional and sector boundaries;
- Work with State, local, tribal, and international governments and the private sector, as appropriate, to evaluate regional and cross-sector CI/KR interdependencies, including cyber considerations;
- Conduct appropriate regional planning efforts and undertake appropriate partnership agreements to enable regional CI/KR protection activities and enhanced response to emergencies;
- Facilitate information sharing and data collection between and among regional initiative members and external partners;
- Share information on progress and CI/KR protection requirements with DHS, the SSAs, the States, and other CI/KR security partners, as appropriate; and
- Participate in the NIPP partnership model, as appropriate.

The Pacific Northwest Economic Region provides an example of a regional organization structured as a public-private partnership that includes legislators, governments, and businesses in five States and three Canadian provinces. The Region, established by statute in all member States and Provinces, sponsors bi-national, multi-jurisdictional CI/KR protection interdependency exercises, and has developed an action plan outlining several physical and cyber CI/KR protection projects with important regional impact.

2.2.4.5 Boards, Commissions, Authorities, Councils, and Other Entities

An array of boards, commissions, authorities, councils, and other entities at the State, local, tribal, and regional levels perform regulatory, advisory, policy, or business oversight functions related to various aspects of CI/KR operations and protection within and across sectors and jurisdictions. Some of these entities are established through State- or local-level executive or legislative mandates with elected, appointed, or voluntary membership. These groups include, but are not limited to: transportation authorities, public utility commissions, water and sewer boards, park commissions, housing authorities, public health agencies, and many others. These entities may serve as SSAs within a State and contribute expertise, assist with regulatory authorities, or help to facilitate investment decisions related to CI/KR protection efforts within a given jurisdiction or geographical region.

2.2.5 Private Sector Owners and Operators

Owners and operators generally represent the first line of defense for the CI/KR under their control. Private sector owners and operators are responsible for taking action to support risk management planning and investments in security as a necessary component of prudent business planning and operations. In today's risk environment, these activities generally include reassessing and adjusting continuity-of-business and emergency management plans, building increased resiliency and redundancy into business processes and systems, protecting facilities against physical and cyber attacks and natural disasters, guarding against the insider threat, and increasing coordination with external organizations to avoid or minimize the impacts on surrounding communities or other industry partners.

For many private sector enterprises, the level of investment in security reflects risk versus consequence tradeoffs that are based on two factors: (1) what is known about the risk environment, and (2) what is economically justifiable and sustainable in a competitive marketplace or in an environment of limited resources. In the context of the first factor, the Federal Government is uniquely postured to help inform critical security investment decisions and operational planning. For example, owners and operators generally look to the government as a source of security-related best practices and for attack indications, warnings, and threat assessments. In relationship to the second factor, owners and operators also generally rely on government entities to address risks outside of their property or in situations in which the current threat exceeds an enterprise's capability to protect itself or mitigate risk beyond a reasonable level of additional investment. In this situation, public and private sector security partners at all levels must collaborate to address the protection of national-level CI/KR, provide timely warning, and promote an environment in which CI/KR owners and operators can better carry out their specific protection responsibilities. Additionally, CI/KR owners and operators may be required to invest in security as a result of Federal, State, and/or local regulations.

The CI/KR protection responsibilities of specific owners or operators vary widely within and across sectors. Some sectors have regulatory or statutory frameworks that govern private sector security operations within the sector; however, most are guided by voluntary security regimes or adherence to

Public Utility Commissions provide an example of a State entity with responsibility for electricity, gas, and telecommunications infrastructures and, in some cases, water, wastewater/sewage, and certain aspects of transportation. As such, Public Utility Commissions are uniquely positioned to deal with the recovery of investments made for protection of critical infrastructure in these areas. Furthermore, Public Utility Commissions historically have been concerned with the adequacy and reliability of these services, and have facilitated investments made by these industries to ensure that they are resilient and reliable.

For example, Public Utility Commissions work together to address issues of mutual concern based on the interdependencies between the water, telecommunications, and energy infrastructures (in the context of preparedness for, and response to, events impacting critical infrastructure) by:

- Creating networks among utility regulators and other Federal, State, local, and private sector entities to address cross-sector issues;
- Exploring and recommending solutions for information disclosure issues (especially protecting sensitive security information from public disclosure while ensuring that all critical stakeholders have access to essential information);
- Exploring and recommending solutions to cost-recovery issues associated with key water, gas, telecommunications, and energy infrastructures; and
- Identifying and prioritizing issues, researching best practices, and disseminating information to Federal and State partners and affiliates.

industry-promoted best practices. Within this diverse protective landscape, private sector entities can better secure the CI/KR under their control by:

- Performing comprehensive risk assessments tailored to their specific sector, enterprise, or facility risk landscape;
- Developing an awareness of critical dependencies and interdependencies at the sector, enterprise, and facility levels;
- Implementing protective actions and programs to reduce identified vulnerabilities appropriate to the level of risk presented;
- Establishing cyber security programs and associated awareness training within the organization;
- Adhering to recognized industry best business practices and standards, including those with a cyber security nexus (see appendix 5B);
- Developing and coordinating CI/KR protective and emergency response actions, plans, and programs with appropriate Federal, State, and local government authorities;
- Participating in the NIPP sector partnership model (including SCCs and information-sharing mechanisms), as appropriate;
- Assisting and supporting Federal, State, local, and tribal government CI/KR data collection and protection efforts, as appropriate;
- Participating in Federal, State, local, and tribal government emergency management programs and coordinating structures;
- Establishing resilient, robust, and/or redundant operational systems or capabilities associated with critical functions where appropriate;
- Promoting CI/KR protection education, training, and awareness programs;
- Adopting and implementing effective workforce security assurance programs to mitigate potential insider threats;
- Providing technical expertise to SSAs and DHS when appropriate;
- Participating in regular CI/KR protection-focused exercise programs with other public and private sector security partners;
- Identifying and communicating requirements to DHS and/or SSAs for CI/KR protection-related R&D;
- Sharing security-related best practices and entering into operational mutual-aid agreements with other industry partners; and
- Working to identify and help remove barriers to public-private partnerships.

2.2.6 Advisory Councils

Advisory councils provide advice, recommendations, and expertise to the government regarding CI/KR protection policy and activities. These entities also help enhance public-private partnerships and information sharing. They often provide an additional mechanism to engage with a pre-existing group of private sector leaders to obtain feedback on CI/KR protection policy and programs, and to make suggestions to increase the efficiency and effectiveness of specific government programs. Examples of CI/KR protection-related advisory councils and their associated responsibilities include:

- Critical Infrastructure Partnership Advisory Council (CIPAC): CIPAC is a partnership between government and private sector CI/KR owners and operators that facilitates effective coordination of Federal CI/KR protection programs. CIPAC engages in a range of CI/KR protection activities such as planning, coordination, NIPP implementation, and operational activities, including incident response, recovery, and reconstitution. DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a Federal Advisory Committee Act (FACA)[18]-exempt body pursuant to section 871 of the Homeland Security Act (see chapter 4).
- Homeland Security Advisory Council (HSAC): The HSAC provides advice and recommendations to the Secretary of Homeland Security on relevant issues. The Council members, appointed by the DHS Secretary, include experts from State and local governments, public safety, security and first-responder communities, academia, and the private sector.
  - Private Sector Senior Advisory Committee (PVTSAC): The Secretary of Homeland Security established the PVTSAC as a subcommittee of the HSAC to provide the HSAC with expert advice from leaders in the private sector.

[18] FACA authorized the establishment of a system governing the creation and operation of advisory committees in the executive branch of the Federal Government and for other purposes. The act, when it applies, generally requires advisory committees to meet in open session and make publicly available associated written materials. It also requires a 15-day notice before any meeting may be closed to public attendance, a requirement which could prevent a meeting on short notice to discuss sensitive information in an appropriate setting.

- National Infrastructure Advisory Council (NIAC): The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber systems across all CI/KR sectors. The Council is comprised of up to 30 members appointed by the President. Members are selected from the private sector, academia, and State and local governments. The Council was established (and amended) under Executive Orders 13231, 13286, and 13385.
- National Security Telecommunications Advisory Committee (NSTAC): The NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing National Security and Emergency Preparedness (NS/EP) communications policy. The NSTAC is comprised of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies. It was created under Executive Order 12382.

2.2.7 Academia and Research Centers

The academic and research center communities play an important role in enabling national-level CI/KR protection and implementation of the NIPP, including:

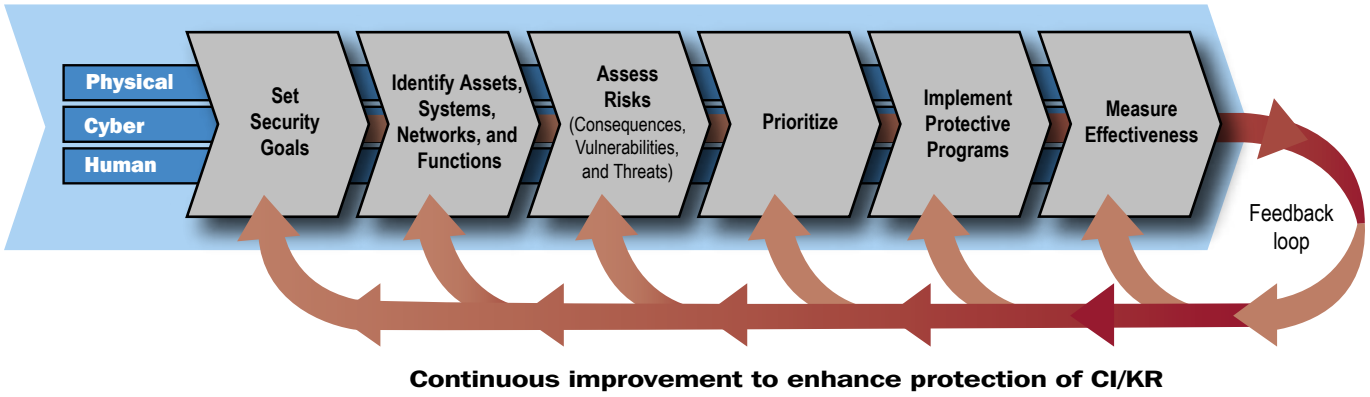
- Establishing Centers of Excellence (i.e., university-based partnerships or federally funded R&D centers) to provide independent analysis of CI/KR protection issues;
- Supporting the research, development, testing, evaluation, and deployment of CI/KR protection technologies;
- Analyzing, developing, and sharing best practices related to CI/KR protection efforts;
- Researching and providing innovative thinking and perspective on threats and the behavioral aspects of terrorism;
- Preparing or disseminating guidelines, courses, and descriptions of best practices for physical security and cyber security;
- Developing and providing suitable security risk analysis and risk management courses for CI/KR protection professionals; and
- Conducting research to identify new technologies and analytical methods that can be applied by security partners to support NIPP efforts.

3. The Protection Program Strategy: Managing Risk

The cornerstone of the NIPP is its risk management framework. Risk is generally defined as the combination of the frequency of occurrence, vulnerability, and the consequence of a specified hazardous event. In the context of the NIPP, risk is the expected magnitude of loss (e.g., deaths, injuries, economic damage, loss of public confidence, or government capability) due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss. The NIPP risk management framework (see figure 3-1) establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector-specific risk that drives CI/KR protection activities. The framework applies to the general threat environment, as well as to specific threats or incident situations. In the case of natural disasters and accidents, the incident management community has access to risk assessment tools such as the models used by the National Hurricane Center (NHC) and the fault trees used by the NRC. Because similar models are not yet in broad use for terrorist threats, the NIPP provides an augmented framework for the terrorist-related aspects of threat analysis.

This chapter addresses the use of the risk management framework as part of the overall effort to ensure a steady-state of protection within and across the CI/KR sectors. DHS, the SSAs, and their security partners share responsibility for implementation of the NIPP risk management framework. SSAs are responsible for leading sector-specific risk management programs and for ensuring that the tailored, sector-specific application of the risk management framework is addressed in their respective SSPs. DHS supports these efforts by providing guidance, tools, and analytical support to SSAs and other security partners. DHS, in collaboration with other security partners, is responsible for using the results obtained in sector-specific efforts to conduct cross-sector risk analysis and management activities. This includes the assessment of dependencies, interdependencies, and cascading effects; identification of common vulnerabilities; development and sharing of common threat scenarios; development and sharing of cross-sector measures to reduce or manage risk; and identification of specific R&D needs.

Figure 3-1: NIPP Risk Management Framework



The risk management framework is tailored and applied on an asset, system, network, or function basis, depending on the fundamental characteristics of the individual CI/KR sectors. For those sectors primarily dependent on fixed assets and physical facilities, a bottom-up, asset-by-asset approach may be most appropriate. For sectors with diverse and logical assets, such as Telecommunications and Information Technology, a top-down, business or mission continuity approach that focuses on networks, systems, and functions may be more effective. Each sector chooses the approach that produces the most actionable results for the sector and works with DHS to ensure that the relevant risk analysis procedures are compatible with the criteria established in the NIPP.

The NIPP risk management framework includes the following activities:

- **Set security goals:** Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.
- **Identify assets, systems, networks, and functions:** Develop an inventory of the assets, systems, and networks, including those located outside the United States, that comprise the Nation's CI/KR and the critical functionality therein; collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.
- **Assess risks:** Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards (including seasonal changes in consequences, and dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.
- **Prioritize:** Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk; and determine protection and business continuity initiatives that provide the greatest mitigation of risk.
- **Implement protective programs:** Select sector-appropriate protective actions or programs to reduce or manage the risk identified; secure the resources needed to address priorities.
- **Measure effectiveness:** Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CI/KR protection program in improving protection, managing risk, and increasing resiliency.

The NIPP is based on the principle of risk management, combining consequence, vulnerability, and threat information. Whether a top-down or bottom-up approach is used, the goal is the same: identify those key assets, systems, networks, and functions most in need of focused risk mitigation measures.

DHS and the SSAs use information from metrics and other evaluation tools to support continuous improvement. Information about the current status of each sector is compared to the baseline of information collected and analyzed during initial risk assessments to measure progress over time. This process forms a feedback loop, which allows the Federal Government and its security partners to track progress and implement actions to improve national CI/KR protection and resiliency.

The physical, cyber, and human elements of CI/KR are considered during each step of the risk management framework. The sector partnership model discussed in chapter 4 provides the structure for coordination and management of risk management activities that are tailored to each sector.

3.1 Set Security Goals

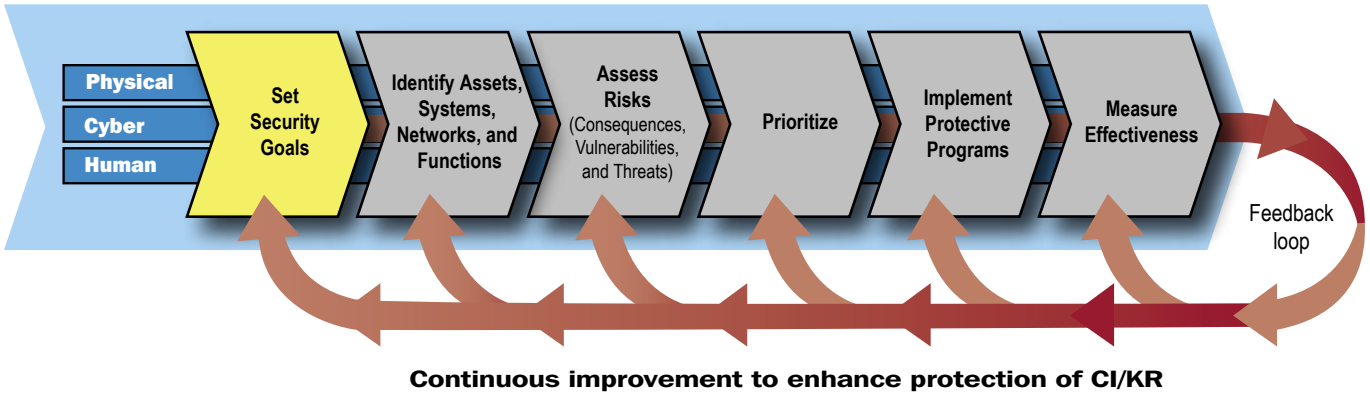
Achieving a robust, protected, and resilient infrastructure requires national and sector-specific homeland security goals that collectively represent the desired security posture. These goals should consider the physical, cyber, and human elements of CI/KR protection. Security goals may vary across and within sectors, depending on the internal structure and composition of a specific industry, resource, or other aspect of CI/KR.

Nationally, the overall goal of risk management efforts is an enhanced state of CI/KR protection achieved through the implementation of focused risk-mitigation and protective strategies within and across sectors. The risk management framework supports this goal by:

Sample Security Goal
Telecommunications Sector

Build networks and systems that provide secure and resilient communications for the Nation and that can be rapidly restored after a natural or manmade disaster.

Figure 3-2: NIPP Risk Management Framework: Set Security Goals



- Supporting the development of the national risk profile presented in the National CI/KR Protection Annual Report described in chapter 7. This is a high-level summary of the aggregate risk and the protective status of all sectors. It is developed by DHS in collaboration with other security partners, updated on an ongoing basis, and used to support strategic decisionmaking, planning, and resource allocation;
- Enabling DHS, SSAs, and other security partners to determine the best courses of action to reduce potential consequences, threats, or vulnerabilities. Some available options include encouraging voluntary implementation of focused risk management strategies (e.g., through public-private partnerships), pursuing economic incentive-related policies and programs, and undertaking regulatory action if appropriate; and
- Using prioritized information to identify, or create, specific protective programs for CI/KR of the highest criticality based on risk. Depending on the protective program, resource allocation may occur at the Federal, State, Territorial, local, or tribal level, or may be solely the responsibility of CI/KR owners and operators. International outreach and collaboration also may be required in many circumstances.

From a sector perspective, security goals or their related supporting objectives:

- Define the protective (and, if appropriate, the response or recovery) posture that security partners seek to attain;
- Express this posture in terms of objective metrics and the time required to attain it through specific supporting objectives;
- Consider distinct assets, systems, networks, operational processes, business environments, and risk management approaches; and
- Vary according to the specific business characteristics and security landscape of the affected sector, jurisdiction, or locality.

Taken collectively, these goals guide all levels of government and the private sector in tailoring protective programs and activities to address CI/KR protection needs.

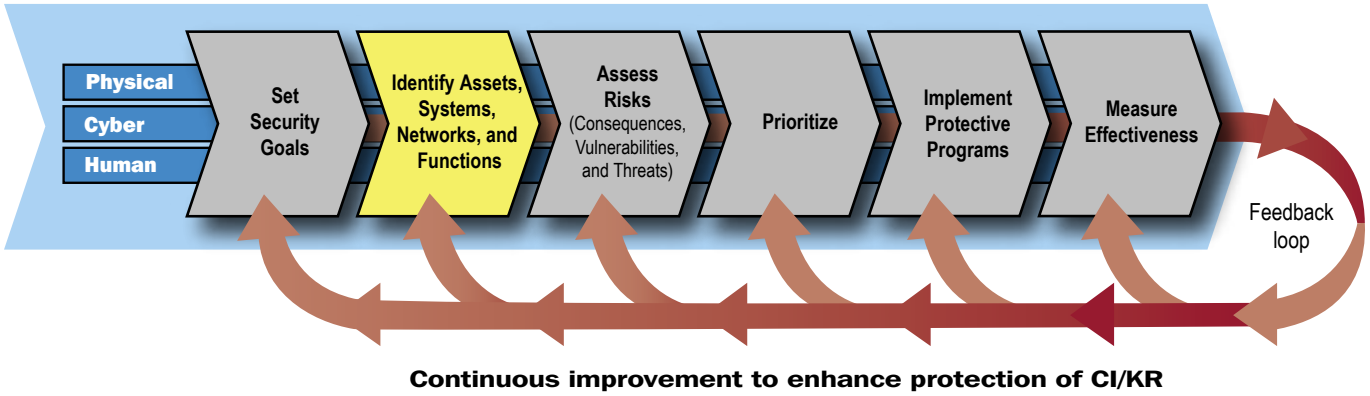
3.2 Identify Assets, Systems, Networks, and Functions

To meet its responsibilities under the Homeland Security Act and HSPD-7, DHS maintains a comprehensive national inventory of the information needed to identify those assets, systems, networks, and functions that make up the Nation's CI/KR. This information may be different for each sector because it is collected on an asset, system, network, or function basis, as determined by the fundamental characteristics of each sector.

3.2.1 National Infrastructure Inventory

The inventory addresses the physical, cyber, and human elements of each asset, system, network, or function under consideration. The compilation process relies on the substantial body of previous assessments that have been completed for natural disasters, industrial accidents, and other incidents. The inventory includes basic information on the relationships, dependencies, and interdependencies between various assets, systems, networks, and functions; on service providers, such as schools and businesses, that may be of relevance

Figure 3-3: NIPP Risk Management Framework: Identify Assets, Systems, Networks, and Functions



to more than one sector; and on the foreign assets, systems, networks, and functions on which U.S. CI/KR may rely. The inventory also includes a cyber data framework that is used to characterize each sector's unique cyber assets, systems, networks, or functions.

DHS compiles the inventory in a manner that enables it to be quickly scanned, searched, and analyzed. This allows DHS to rapidly identify those assets, systems, networks, or functions at greatest risk in different situations. For example, the information may be used to quickly identify those assets, systems, networks, or functions that may be the subject of emergent terrorist statements or interest or that may be located in the area of greatest impact from natural disasters.

This information is needed not only to help manage steady-state CI/KR protection and resiliency approaches, but also to inform and support the response to a wide array of incidents and emergencies. Risk may change based on many factors including damage resulting from a natural disaster; seasonal or cyclic dependencies; and changes in technology, the economy, or the terrorist threat. The inventory is used to support domestic incident management by helping to inform decisionmaking; establish strategies for response; and identify priorities for restoration, remediation, and reconstruction.

Currently, this inventory is maintained in the NADB. SSAs and DHS work together and in concert with State, local, and tribal governments, and private sector security partners to ensure that the inventory data structure is accurate, current, and secure. DHS provides guidelines concerning information needed to develop and maintain the inventory. Owners, operators, infrastructure data source managers, and other security partners generally have the best knowledge of their assets, systems, networks, functions, and related data. These subject matter experts work with DHS and the SSAs to determine the specific information required to support sector and national-level risk analysis. Judgments on the information to be provided for DHS use is informed by a screening process (described in section 3.3.2.2). The screening process applies an essential needs test that considers the consequences that would result if an asset, system, network, or function were lost, exploited, damaged, or disrupted.

For sectors with identifiable facilities, a bottom-up, asset-based approach often is most appropriate for collecting and organizing inventory information; for sectors with virtual- or information-based core processes, a top-down system-, network-, or function-based approach may be more appropriate. A bottom-up approach normally includes an aggregate assessment at the individual facility level; this is with regard to both on-site and off-site consequences to the facility's mission and the surrounding population that could result from natural disasters, accidents, or terrorist attacks. A top-down approach normally includes an assessment of key missions and the identification of the high-level processes, capabilities, and functions on which those missions depend; it considers dependencies on other sectors to evaluate resiliency, redundancy, and recoverability. Both the top-down and bottom-up approaches recognize that effects on customers, key users, and the public must be considered in the assessment process to understand what is critical.

Information included in the inventory comes from a variety of sources, such as:

- **Sector inventories:** SSAs maintain close working relationships with owners and operators, SCCs, and other sources that maintain inventories necessary for the sector's business or mission. SSAs provide relevant information to DHS and update it on a periodic basis to ensure that sector assets and critical functions are adequately represented, and that sec-

tor and cross-sector dependencies and interdependencies can be identified and analyzed;

- **Voluntary submittals from security partners:** Owners and operators; State, local, and tribal governments; and Federal departments and agencies voluntarily submit information and previously completed inventories for DHS to consider;
- **Results of studies:** Various government or commercially owned databases developed as the result of studies undertaken by trade associations, advocacy groups, and regulatory agencies may contain relevant information;
- **Periodic data calls:** DHS, in cooperation with SSAs and other security partners, may conduct data calls requesting the voluntary provision of specific information; and
- **Ongoing reviews of particular locations where risk is believed to be higher:** DHS- and SSA-initiated site assessments provide information on vulnerability; help to identify assets, systems, and networks and their dependencies, interdependencies, and critical functionality; and quantify their value relative to the potential consequences of an attack.

DHS, in coordination with SSAs, State and local governments, private sector owners and operators, and other security partners, uses consistent reporting methods to gather appropriate basic information for a range of assets, systems, networks, and critical functions in each sector. This approach relies on existing inventories at the State and local levels to avoid duplication of past efforts. To help ensure currency and accuracy, DHS documents the sources of the information maintained in the inventory. DHS also coordinates with security partners, as needed, to gather additional information for assets, systems, networks, and functions that, based on an initial screening, DHS determines to be potentially nationally critical. This additional information may include:

- System components that are central to the infrastructure mission and function;
- Dependencies and interdependencies (i.e., what an asset depends on in order to function, and which assets are reciprocally dependent upon it);
- Specific information on the asset, system, network, or function needed to support consequence analysis; and
- Assessment information that would enable DHS to conduct further comparative risk analysis in cooperation with the SSAs, the private sector, other security partners, or subject matter experts.

3.2.2 Protecting and Accessing Inventory Information

The Federal Government recognizes the sensitive, business, or proprietary nature of much of the information to be included in the NADB. DHS is responsible for protecting this information from unauthorized disclosure or use. Submissions of asset information for inclusion in the NADB are protected from unauthorized disclosure or use to the maximum extent allowed under applicable Federal, State, or local regulation, including PCII and security classification rules (see section 4.3). Additionally, DHS ensures that all data and licensing restrictions are enforced. DHS has implemented resilient and redundant security measures that apply to the NADB; these provide for system integrity and security, software security, and protection of the data therein.

Access to the NADB is tightly controlled using relevant security clearances and classification guidelines. All users must apply for and be approved for access to the NADB based on appropriate authorization, clearance, and a need to know. Once this information is submitted, DHS verifies clearances and need to know, and assigns each individual role-based access authorization based on the scope of the information requested and required.

3.2.3 SSA Roles in Inventory Development and Maintenance

The specific processes that SSAs use to collect asset, system, and network data; to identify critical functionality; and to coordinate with DHS are described in the individual SSPs. The SSPs include descriptions of mechanisms for making data collection efforts more manageable, such as:

- Prioritizing the approach for data outreach to different security partners;
- Identifying assets, systems, networks, or functions of potential national-, regional-, or sector-level importance;
- Identifying, reviewing, and using existing databases;
- Supporting State, local, and tribal entities in gathering information by helping them identify the types of information most relevant to the protection of potentially high-risk infrastructure; and
- Identifying specific assets, systems, or networks, or classes of assets, systems, or networks, for which additional data collection is unnecessary because of the inherently low risk associated with them.

SSAs help identify and obtain appropriate data for assets, systems, networks, and functions that play a vital role in the Nation's security or economy, particularly those that involve significant dependencies, interdependencies, or critical functionality. For example, a small manufacturer of pharmaceuticals or vaccines could be the sole U.S. manufacturer of that product. Similarly, virtual networks, known only to the owner and operator of a communications service, could provide the only sufficiently capable link between the military and the producer of a defense system component. The identification of less visible assets makes the effort more time-consuming; however, it is a crucial part of the process if a true national risk profile is to be developed. More details on SSA roles and responsibilities, as well as those of other security partners, in creating and maintaining the national CI/KR inventory are contained in appendix 3C.

3.2.4 State Roles in Inventory Development and Maintenance

States often have access to sector-specific information maintained by State regulatory agencies that may be appropriate for use in a national CI/KR inventory. States also may have developed CI/KR inventories in conjunction with other responsibilities, such as incident management and response, economic development, and the oversight of commerce and communications. Because of their CI/KR-related responsibilities and authorities, States provide information that is essential in helping to identify and obtain data about assets, systems, and networks that relate to cross-sector matters.

The State homeland security programs should include descriptions of mechanisms that align with those outlined for the SSAs (see section 3.2.3) and that make data collection efforts more manageable. Additional information on State roles and responsibilities in this area is contained in appendix 3C.

3.2.5 Identifying Cyber Infrastructure

The NIPP addresses the protection of the cyber elements of CI/KR in an integrated manner rather than as a separate consideration. As a component of the sector-specific risk assessment process, cyber infrastructure (assets, systems, networks, and functions) should be identified individually or included as a cyber element of a larger asset, system, or network's description if they are associated with one. The identification process should include information on international cyber infrastructure with cross-border implications, interdependencies, or cross-sector ramifications. The following list provides examples of cyber assets, systems, or networks that exist in most, if not all, sectors:

- **Business Systems:** Cyber systems used to manage or support common business processes and operations. Examples of business systems include Enterprise Resource Planning, e-commerce, e-mail, and R&D systems.
- **Control Systems:** Cyber systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. Control systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of control systems include SCADA, Process Control Systems, and Distributed Control Systems.
- **Access Control Systems:** Cyber systems allowing only authorized personnel and visitors physical access to defined areas of a facility. Access control systems provide monitoring and control of personnel passing throughout a facility by various means, including electronic card readers, biometrics, and radio frequency identification.
- **Warning and Alert Systems:** Cyber systems used for alerting and notification purposes in many security missions, including homeland security. These systems pass critical information that triggers protection and response actions for formal organizations and individual citizens. Examples include local phone-based hazard alerting systems used by some local governments and the Emergency Alert System established by the Federal Communications Commission (FCC), and its National Oceanic and Atmospheric Administration Weather Radio, which is an all-hazards alerting system provided by the Department of Commerce.

The Internet has been identified as a key resource comprised of domestic and international assets within both the Information Technology and Telecommunications sectors, and is used by all sectors to varying degrees. While the availability of the service is the responsibility of both the Information Technology and Telecommunications sectors, the need for access to and reliance on the Internet is common to all sectors.

DHS supports SSAs and other security partners by developing tools and methodologies to assist in identifying cyber assets, including those that involve multiple sectors. As needed, DHS works with sector representatives to help identify cyber infrastructure within the NIPP risk management framework. For example, DHS collaborates with the Department of Education in addressing cyber protection and resiliency for schools.

3.2.6 Identifying Positioning, Navigation, and Timing Services

Space-based and terrestrial positioning, navigation, and timing services are a component of multiple CI/KR sectors. These services underpin almost every aspect of transportation across all its various modes. Additionally, the Banking and Finance, Telecommunications, Energy, and Water sectors rely on GPS as their primary timing source. The systems that support or enable critical functions in the CI/KR sectors should be identified, either as part of or independent of the infrastructure, as appropriate. Examples of CI/KR functions that depend on positioning, navigation, and timing services include: aviation (navigation, air traffic control, surface guidance); maritime (harbor, inland waterway vessel movement); surface transportation (rail, hazmat tracking); communications networks (global fiber and wireless networks); and power grids.

3.3 Assess Risks

Various methodologies are available to facilitate risk assessment. Many owners and operators use a risk assessment methodology as a component of their business continuity and disaster mitigation planning. A common approach based on a robust understanding of existing methodologies is needed to enable the setting of protection priorities across sectors. The first element of this approach is to establish a common definition and process for analysis of the basic factors of risk for CI/KR protection. In the context of homeland security, the NIPP framework assesses risk as a function of consequence, vulnerability, and threat:

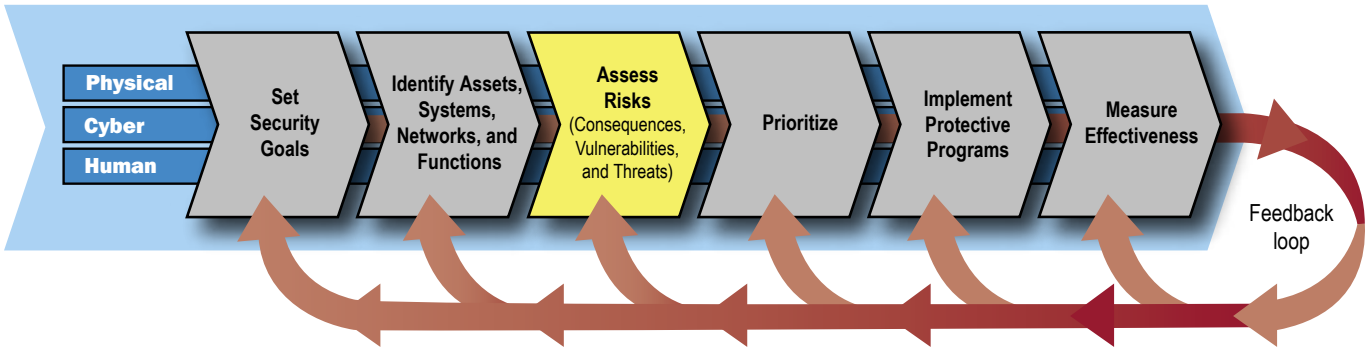
$$R = f(C,V,T)$$

- **Consequence:** The negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident;
- **Vulnerability:** The likelihood that a characteristic of, or flaw in, an asset, system, or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards; and
- **Threat:** The likelihood that a particular asset, system, or network will suffer an attack or an incident. In the context of risk from terrorist attack, the estimate of this is based on the analysis of the intent and the capability of an adversary; in the context of natural disaster or accident, the likelihood is based on the probability of occurrence.

Risk assessments for CI/KR protection consider all three components of risk and are conducted on an asset, system, network, or function basis, depending on the fundamental characteristics of the infrastructure being examined. For some sectors, particularly those with specifically identifiable facilities that might be exploited, an asset-based approach is typically used; for others, particularly those with virtual- or information-based core processes, assessing system or network risk and resiliency is more appropriate.

Once the three components of risk—consequence, vulnerability, and threat—have been assessed for a given asset, system, or network by sector, region, or nationally, they are factored numerically and combined mathematically to give an estimate of the expected loss considering the likelihood of an attack or other incident. Calculating a numerical risk score using comparable, credible methodologies provides a systematic and comparable estimate of risk that can help inform national and sector-level risk management decisions.

Figure 3-4: NIPP Risk Management Framework: Assess Risks



DHS works with the SSAs, State and local governments, private industry, and other security partners to develop an approach that allows risk-based comparisons across sectors, while leveraging assessments and analyses that have already been performed. This approach involves two parallel, mutually supportive efforts:

- Reconfiguring existing, widely used methodologies, or identifying clear and understandable means for making the results of assessments performed using those methodologies comparable with minimal additional cost to security partners; and
- Collaboratively developing a risk assessment process and methodology generally applicable across all sectors that owners and operators will be encouraged to use on a voluntary basis. Owners and operators who might find voluntary use advantageous are those who:
  - Have not previously performed a thorough risk assessment;
  - Wish to streamline their communications with other security partners;
  - Need to update a previously completed assessment; or
  - Would like to use the primary DHS methodology because of the level of support that is available from DHS.

The NIPP establishes baseline criteria for risk assessment methodologies. These criteria provide a guide for improving existing methodologies or modifying them so the investment and expertise they represent can be used to support national-level, comparative risk assessment, planning, and resource prioritization.

DHS is sponsoring the development of a suite of tools based on the Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework that satisfies the baseline criteria for risk assessment and can be used for national cross-sector risk assessment. This tool set enables owners and operators to calculate potential consequences and vulnerability to an attack using a consistent system of measurements. It will also provide the means to convert and compare the results obtained from assessments performed with other suitable methodologies that are consistent with the NIPP baseline criteria.

The NIPP baseline criteria are set forth in the next section. The processes for assessing, analyzing, and combining the three specific components that make up risk—consequence, vulnerability, and threat—are explained in the following sections. More details regarding the baseline criteria are included in appendix 3A.

3.3.1 NIPP Baseline Criteria for Assessment Methodologies

Many owners and operators regularly perform vulnerability or risk assessments on the assets, systems, and networks under their control. To take advantage of this existing body of work, DHS plans to make every effort to use the results from previously performed assessments wherever possible. However, it should be noted that work on assessments to date has varied widely both within and across sectors in terms of assumptions, comprehensiveness, objectivity, and the inclusion of threat and consequence considerations, as well as information regarding physical/cyber dependencies and interdependencies.

3.3.1.1 Ensuring That Previous Assessments Can Be Used

To be accepted by DHS, existing risk assessment tools and methodologies are reviewed against the NIPP baseline criteria. This review helps ensure that the tools provide results that are suitable for national-level risk analysis, which relies on assessments that are comparable both within and across sectors. DHS and the SSAs will work with security partners to ensure that risk assessment tools and methodologies that are compatible with the NIPP criteria are available to security partners. DHS will leverage and incorporate work already done, to the greatest extent possible, and will help tailor existing tools to meet the baseline criteria as required.

3.3.1.2 Baseline Criteria

The NIPP baseline criteria for assessment methodologies fall into two groups; these criteria are described below and listed specifically in appendix 3A.

The first group provides factors to ensure that the methodology is *credible* to users of the resulting analysis. To be considered credible, a methodology must have a sound basis (it must have integrity); be complete; be based on assumptions and produce results that are defensible; and specifically address the three variables of the risk calculus: consequences, vulnerability, and threat.

The second group ensures that the methodology supports a comparative sector or national risk assessment. To be comparable, a methodology must be documented, transparent, reproducible, and accurate. The methodology must also provide clear and sufficient documentation of the analysis process and the products that result from its use.

3.3.2 Consequence Analysis

The potential consequences of any incident, including terrorist attacks and natural or manmade disasters, is the first factor to be considered in risk assessment. In the context of the NIPP, consequence is measured as the range of loss or damage that can be expected.

The consequences that are considered for the national-level comparative risk assessment are based on the criteria set forth in HSPD-7. These criteria can be divided into four main categories:

- **Human Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries);
- **Economic Impact:** Direct and indirect effects on the economy (e.g., cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from disruption of product or service, long-term costs due to environmental damage);
- **Impact on Public Confidence:** Effect on public morale and confidence in national economic and political institutions; and
- **Impact on Government Capability:** Effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

A full consequence assessment takes into consideration public health and safety, economic, psychological, and government impacts; however, estimating potential indirect impacts requires the use of assumptions and other complex variables. An assessment of all categories of consequence may be beyond the capabilities available for a given risk analysis. At a minimum, assessments should focus on the two most fundamental impacts: the human and the most relevant direct economic impact.

3.3.2.1 Consequence Assessment Methodologies That Enable National Risk Analysis

DHS works with SSAs and other security partners to examine the inherent characteristics of assets, systems, or networks to identify worst-case consequences that are likely to result if the CI/KR in question is destroyed, incapacitated, or exploited. The use of common terminology and metrics when assessing consequences supports comparative risk analysis at the national level. DHS works with security partners to develop consequence assessment methodologies that can be applied to a variety of asset, system, or network types and produce comparable quantitative consequence estimates. DHS is working with industry partners to develop a framework for consequence assessment methodologies for selected CI/KR sectors and subsectors. When fully developed and implemented, the methodologies developed under the RAMCAP framework will provide quantitative results that can be compared to the results of any other RAMCAP consequence assessment, regardless of asset type.

Consequence analysis should address both direct and indirect effects. Many assets depend on multiple inputs to maintain functionality. For example, nearly all sectors rely on the Energy, Information Technology, Telecommunications, Banking and Finance, and Transportation sectors. In some cases, a failure of an asset in one sector can have a significant impact on the ability of an asset in the same or another sector to perform necessary functions. As a result, comprehensive consequence analysis addresses both CI/KR dependency (reliance on another asset or sector for functionality) and CI/KR interdependency (when two or more assets depend on one another) for the purposes of NIPP risk assessment.

Various Federal and State entities, including national laboratories, are developing sophisticated models and simulations to identify dependencies and interdependencies within and across sectors. The Federal Government established the National Infrastructure Simulation and Analysis Center (NISAC) to support these efforts. The NISAC is chartered to develop advanced modeling, simulation, and analysis capabilities for the Nation's CI/KR. These tools address physical and cyber dependencies and interdependencies in an all-hazards context. These sophisticated models enhance the Nation's understanding of CI/KR dependencies and interdependencies, and better inform decisionmakers in the areas of policy analysis, investment, prevention and mitigation planning, education, training, and crisis response.

The level of detail and specificity achieved by using the most sophisticated models and simulations may not be practical or necessary for some assets, systems, or networks. In these circumstances, a simplified dependency and interdependency analysis based on expert judgment may be used to provide the insight necessary to make informed risk management decisions in a timely manner.

3.3.2.2 Consequence Screening

Many risk assessment methodologies use a simplified and inexpensive-to-use consequence screening, or top-screens, to help owners and operators decide whether a full risk assessment is necessary. For example, DHS uses sector-specific top-screens as part of the RAMCAP framework. This approach allows CI/KR owners and operators to identify their projected level of consequence based on the nature

of their business, proximity to significant populations or other CI/KR, relative importance to the national economy or military capability, and other similar factors. The screening process uses a standard form containing a few simple questions. If this initial screening determines that an attack on an asset, system, or network is likely to result in consequences that are considered low from a national perspective, owners and operators will not be asked to provide additional information to DHS or SSAs. However, assets, systems, or networks that are screened out because of their relatively low national risk may be considered critical on a sector or jurisdictional basis (e.g., a chemical facility that is the primary employer in a given community). Accordingly, additional analysis may be warranted. Owners and operators of CI/KR that are screened out using a consequence screening assessment should consider whether their assets, systems, or networks require more detailed assessments in conjunction with other State, regional, or local CI/KR protection efforts.

3.3.3 Vulnerability Assessment

Vulnerabilities are the characteristics of an asset, system, or network's design, location, security posture, process, or operation that render it susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks, or other malicious acts. They identify areas of weakness that could result in consequences of concern, taking into account intrinsic structural weaknesses, protective measures, resiliency, and redundancies.

The vulnerability assessment process typically consists of the following key steps:

- Determining an appropriate vulnerability assessment strategy (e.g., self-assessment, State- or federally led assessment, expert reviews, or independent third-party assessment);
- Identifying a methodology/tool appropriate for the particular type of asset, system, or network under consideration;
- Identifying and grouping vulnerabilities using common threat scenarios;
- Identifying dependencies and interdependencies with other assets and sectors;
- Considering vulnerabilities associated with physical, cyber, and human elements;
- Analyzing benefits of existing protective programs; and
- Assessing residual gaps to determine unresolved vulnerabilities.

3.3.3.1 Vulnerability Assessment Methodologies That Enable National Risk Analysis

Many different vulnerability assessment approaches are used by the different CI/KR sectors. The primary vulnerability assessment methodologies used in each sector are described in the respective SSPs. The SSPs also provide specific detail regarding how the assessments can be carried out (e.g., by whom, how often).

The results of vulnerability assessments need to be comparable in order to support further national-level, cross-sector analysis. DHS, in conjunction with various security partners, continuously improves vulnerability methodologies developed under the RAMCAP framework. This provides two means for producing comparable vulnerability assessment results. First, as part of the framework, DHS develops sector-specific Security Vulnerability Assessment (SVA) modules for individual sectors and subsectors. These SVA modules use a common approach that produces results that may be compared with other SVA module assessment results. Second, as part of the development of each SVA module, DHS and its security partners review vulnerability assessment methodologies that are used in the specific sector or subsector, and assess their compatibility with the NIPP baseline criteria. If methodologies conform to the baseline criteria, then DHS can use assessment results produced using that methodology to support national comparative risk analysis. If the methodologies differ, DHS will work with security partners to either identify ways to adjust the methodology to conform to the NIPP baseline criteria, or will develop "translators" to convert results developed with those methodologies into results that are comparable with the SVA modules. The specific approach will depend on the degree of difference and the robustness of the method in question.

3.3.3.2 SSA and DHS Analysis Responsibilities

SSAs and their security partners are responsible for taking stock of, and facilitating, vulnerability assessment activities within their sectors; owners or operators typically perform these assessments. SSAs are also responsible for compiling, where possible, vulnerability assessment results for use in sector and national risk management efforts. Vulnerability assessment information may be submitted under the PCII Program (see Section 4.3, Protection of Sensitive CI/KR Information). SSAs are responsible for working with DHS to validate the results of those assessments for assets that are of the greatest concern from the sector perspective. SSAs should involve owners and operators in this review whenever possible.

DHS is responsible for ensuring that comprehensive vulnerability assessments are performed for CI/KR that is deemed

nationally critical. This may involve DHS experts performing the vulnerability assessment in conjunction with the CI/KR owner or operator, or working with the CI/KR owner or operator, the SSA, or a third-party auditor to perform or to verify previously performed assessments.

DHS also conducts or supports vulnerability assessments that address the specific needs of the NIPP's comprehensive approach to CI/KR protection. Such assessments may:

- More fully investigate dependencies and interdependencies within and between sectors;
- Serve as a basis for developing common vulnerability reports that can help identify strategic needs for protective programs or R&D across sectors or subsectors;
- Fill selected gaps when sectors or owners or operators have not yet completed assessments and such studies are needed immediately; and
- Test and validate new methodologies or streamlined approaches for assessing vulnerability.

In some sectors and subsectors, vulnerability assessments have never been performed or may have been performed for only a small number of high-profile or high-value assets, systems, or networks. To help assist in closing this gap, DHS works with SSAs, and owners and operators, as well as other security partners, as appropriate, to determine common criteria for vulnerability assessments and provides:

- Vulnerability assessment tools that may be used as part of self-assessment processes;
- Informative reports for industrial sectors, classes of activities, and high-consequence or at-risk special event sites;
- Generally accepted risk assessment principles for major classes of activities and high-consequence or at-risk special event sites;
- Assistance in the development and sharing of industry-based standards and tools;
- Recommendations regarding the frequency of assessments, particularly in light of emergent threats;
- Site assistance visits and vulnerability assessments of specific CI/KR of particular concern as requested by owners and operators; and
- Cross-sector cyber vulnerability assessment best practices.

3.3.4 Threat Analysis

The remaining factor to be considered in the NIPP risk assessment process is the analysis of threat. In the context of terrorist risk assessment, the threat component of the analysis is calculated based on the likelihood of a terrorist attack method on a particular asset, system, or network.[19] The estimate of this likelihood is based on an analysis of intent and capability of a defined adversary, such as a terrorist group. In the context of a natural disaster or accident, the likelihood is based on the probability of occurrence. The incident management, disaster response, public safety, and other communities have developed and use various tools to estimate the threat of natural disasters and accidents. These tools include such analytical aids as the models used by the NHC to forecast hurricane landfall and the fault tree models used by the NRC in nuclear power plant engineering analysis. Because similar models are not yet in broad use for terrorist threats, the NIPP provides an augmented framework for the terrorist aspects of threat analysis.

Assessment of the current terrorist threat to the United States is derived from extensive study and understanding of terrorists and terrorist organizations, and frequently is dependent on analysis of classified information. DHS, to the greatest extent possible, provides its security partners with Federal Government-coordinated unclassified assessments of potential terrorist threats and appropriate access to classified assessments where necessary. These threat assessments are derived from analysis of adversary intent and capability, and describe what is known about terrorist interest in particular CI/KR sectors, as well as specific attack methods. Since international terrorists, in particular, have continually demonstrated flexibility and unpredictability, DHS and its partners in the Intelligence Community also analyze known terrorist goals and capabilities to provide CI/KR owners and operators with a broad view of the potential threat and postulated terrorist attack methods.

3.3.4.1 Key Aspects of the Terrorist Threat to CI/KR

Analysis of terrorist goals and motivations identify domestic and international CI/KR as potentially prime targets for terrorist attack; given the deeply rooted nature of these goals and motivations, CI/KR likely will remain a highly attractive target for terrorists for some time to come. The characteristics of each of the elements of CI/KR—physical, cyber, and human—relate to attack modalities that risk-mitigation measures must address. Physical attacks, including the exploitation of physical elements of CI/KR, represent the attack method most frequently used overtly by terrorists.

[19] In calculations for risk analysis, the term "threat" is an estimated value that approximates the likelihood that a specific asset, system, network, sector, or region will suffer an attack or an incident. This differs from "threat scenarios," or "threat analysis," which are generalized descriptions of potential methods of attack that are used to help inform consequence and vulnerability assessments.

In addition to physical attacks, terrorists may use the cyber domain as a platform to attack America's CI/KR. The use of innovative technology and interconnected networks in CI/KR operations improves productivity and efficiency, but also may increase the Nation's risk to cyber attacks. Because of the interconnected nature of the cyber elements of CI/KR, cyber attacks can spread quickly and could have a substantial impact on the Nation's essential services and functions. Credible information on specific adversaries or attack modalities frequently is not available in the context of cyber threats. However, the rapidly changing technology and the relatively easy access to and use of powerful cyber tools raises the likelihood that adversaries can develop the capability to conduct cyber attacks against CI/KR. Cyber threats are addressed in unclassified documents such as the *National Strategy to Secure Cyberspace* as well as classified reports such as the *National Intelligence Estimate of Cyber Threats to the U.S. Information Infrastructure*.

A third important aspect in this element of risk is the long-standing threat posed by insiders, or persons who have access to sensitive information and facilities. Insider threats can result from intentional actions, such as infiltration of the organization by terrorists, or unintentional actions, such as employees who are exploited or unknowingly manipulated to provide access to, or information about, CI/KR. Insiders can intentionally compromise the security of CI/KR through espionage, sabotage, or other harmful acts motivated by the rewards offered to them by a terrorist or other party. Others may provide unwitting assistance to an insider threat through lack of awareness of the need for or methods to protect assets or employees (e.g., by leaving security badges and uniforms in open areas). CI/KR owners and operators and authorities with protection responsibilities screen and, if necessary, monitor employees in sensitive positions. These efforts often benefit from the support of Federal regulations and programs that relate to security clearances, and employment-related screening. Examples include industrial security clearance programs, managed by DOD, and screening for personnel afforded unescorted access to commercial aircraft or secure areas at airports, overseen by the Transportation Security Administration (TSA).

3.3.4.2 Homeland Infrastructure Threat and Risk Analysis Center

The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts integrated threat analysis for all CI/KR sectors. As called for in section 201 of the Homeland Security Act, HITRAC brings together intelligence and infrastructure specialists to ensure a complete and sophisticated understanding of the risks to U.S. CI/KR. HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement to integrate and analyze intelligence and law enforcement information on the threat. It also works in partnership with the SSAs and owners and operators to ensure that their expertise on infrastructure operations is integrated into threat analysis. This coordination is carried out through a number of mechanisms, including the use of liaison personnel from the private sector, the use of on-call subject matter experts, and coordination with existing organizations such as National Coordinating Center for Telecommunications (NCC) and the SCCs or Information Sharing and Analysis Centers (ISACs) discussed in chapter 4.

As shown in figure 3-5, HITRAC develops analytical products by combining intelligence expertise based on all-source information, threat assessments, and trend analysis with practical business and CI/KR operational expertise informed by current infrastructure status and operations information. This comprehensive analysis provides an understanding of the threat, CI/KR vulnerabilities, the potential consequences of attacks, and the effects of risk-mitigation actions on not only the threat, but also on business and operations. This combination of intelligence and practical knowledge allows HITRAC to provide CI/KR risk assessment products that contain strategically relevant and actionable information. It also allows HITRAC to identify intelligence collection requirements in conjunction with owners and operators so that the intelligence community can provide the type of information necessary to support the CI/KR protection mission. HITRAC coordinates closely with security partners outside the Federal Government through the SCCs, GCCs, and ISACs to ensure that its analytic products are relevant to security partner needs, and that they are accessible to the partners who need them.

Based on HITRAC analysis, DHS produces two classes of information that support the NIPP:

- Information that supports responses to emergent threats or immediate incidents; and
- Information that supports the strategic planning needed to enhance the protection of U.S. CI/KR over the long term.

Each of these classes of information and the specific DHS products that they include are discussed below.

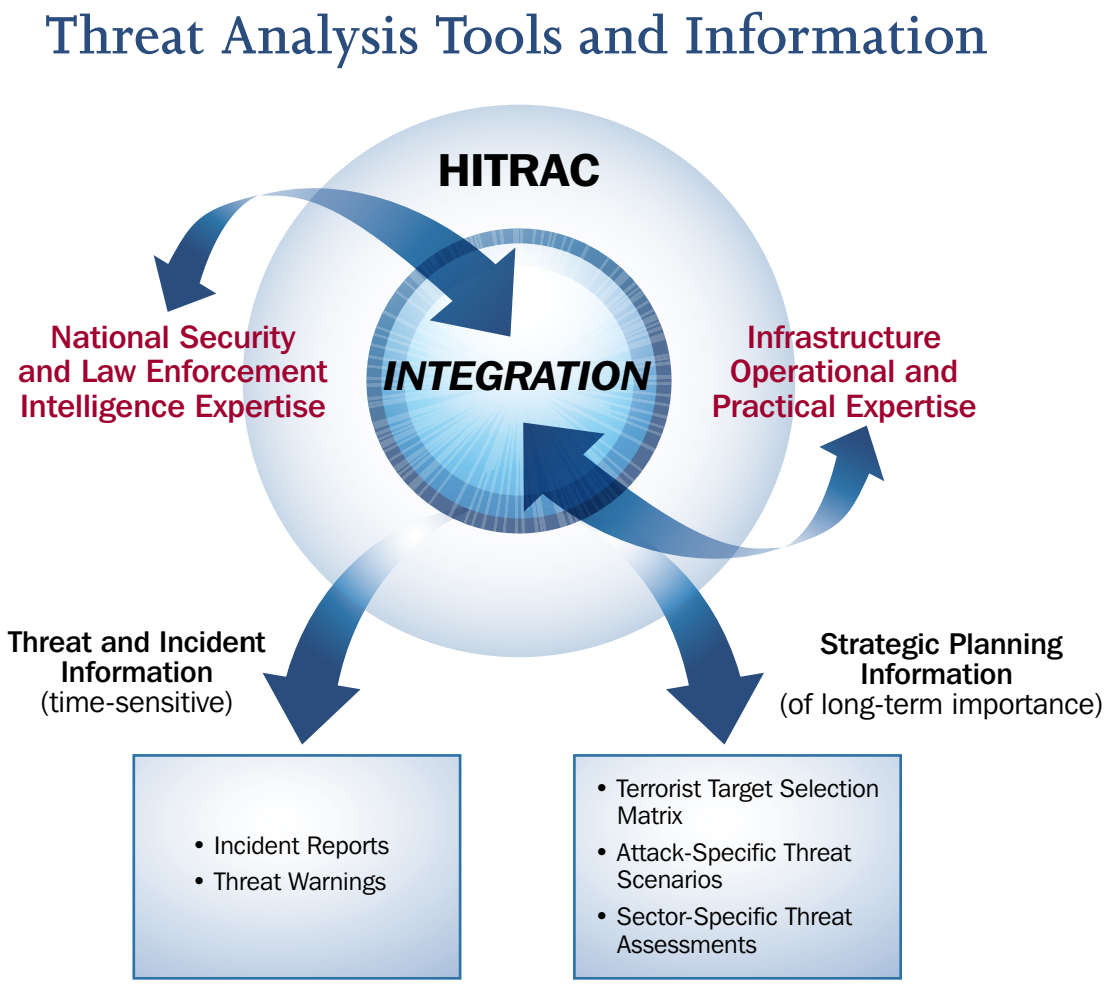
Threat and Incident Information: DHS leverages 24/7 intelligence and operations monitoring and reporting from multiple sources to provide analysis that is based on the most current information available on threats, incidents, and infra-

structure status. Real-time analysis of threat, situation, and CI/KR status information provided by DHS is of unique value to security partners and helps them determine if changes are needed in steady-state CI/KR risk management measures.

Specialized products that directly support the NIPP and SSPs include incident reports and threat warnings, which are made available to appropriate security partners.

- **Incident Reports:** DHS monitors information on incidents to provide reports that CI/KR owners and operators and other decisionmakers can use with confidence when considering how evolving incidents might affect their security posture. This reporting provides a responsive and credible source to verify or expand on information that security partners may receive initially through news media, the Internet, or other sources. DHS works with multiple government and private sector operations and watch centers to combine situation reports from law enforcement, intelligence, and private sector sources with infrastructure status and operational expertise to rapidly produce reports from a trusted source. These help inform the decisions of owners and operators regarding changes in risk-mitigation measures that are needed to respond to incidents in progress, such as rail or subway bombings overseas that may call for precautionary actions domestically.
- **Threat Warnings:** DHS fuses all-source information to provide analysis of emergent threats on a timely basis. Many of the indicators that are reported by intelligence or law enforcement are not associated with an incident in progress, but are the product of careful intelligence collection. Such indicators also may be of significance only when interpreted in the context of infrastructure operational or status information. DHS monitors the flows of intelligence, law enforcement, and private sector security information on a 24/7 basis in light of the business, operational,

Figure 3-5: Threat Analysis Combines Intelligence and Infrastructure Expertise to Provide Threat and Incident Information and Strategic Planning Information



and status expertise provided by its owner and operator security partners to produce relevant threat warnings for CI/KR protection. This analysis clarifies the implications of intelligence reporting about targeted locations or sectors, potential attack methods and timing, or the specific nature of an emerging threat.

- **Strategic Planning Information:** HITRAC analyzes information about terrorist goals, objectives, and attack capabilities to assess the potential terrorist attack profiles that might be used against each CI/KR sector. This provides the best-informed estimate of the potential threat, and is used as a supplement to, or in the absence of, specific intelligence and warnings regarding particular targets, attack vectors, or timing. This analysis provides decisionmakers with the broad, analytically based information on the threat that is necessary to inform investment priorities and program design in conjunction with strategic planning. It also provides the overarching analytic foundation for incident reports and threat warnings produced by DHS and other Federal partners.

HITRAC also develops specialized products for strategic planning that directly support the NIPP and SSPs. These products include a terrorist target selection matrix, which outlines plausible means of attack for each of the CI/KR sectors, a catalog of attack-specific scenarios, and a sector-specific threat report that provides detailed information on the estimated threat facing each sector. In addition to these specific products, HITRAC produces special, longer term strategic assessments and trends analyses that help define the evolving threat to the Nation's CI/KR.

- **Terrorist Target Selection Matrix:** DHS provides threat assessments to SSAs, CI/KR owners and operators, and other security partners who require them. It uses the Terrorist Target Selection Matrix produced by HITRAC as an analytical tool for identifying which sectors are potentially prone to different terrorist attack modalities.

  The matrix maps terrorist goals and objectives against an array of possible attack modalities on a sector-by-sector basis. If intelligence analysis of terrorist intent and capabilities determines that terrorists are unlikely to use particular attack methods against a specific CI/KR sector or subsector, it is noted as an unlikely possibility and further consequence or vulnerability assessment may not be warranted. If a combination is determined to meet only one or two primary terrorist attack objectives, the sector is rated as modestly attractive as a terrorist target. If terrorists can achieve a majority of their objectives by using a particular attack method against a sector or subsector, the situation warrants careful attention and priority for consequence and vulnerability assessments.

  This product supports national-level risk assessments, sector-specific application of the NIPP risk management framework, and development and implementation of the SSPs.

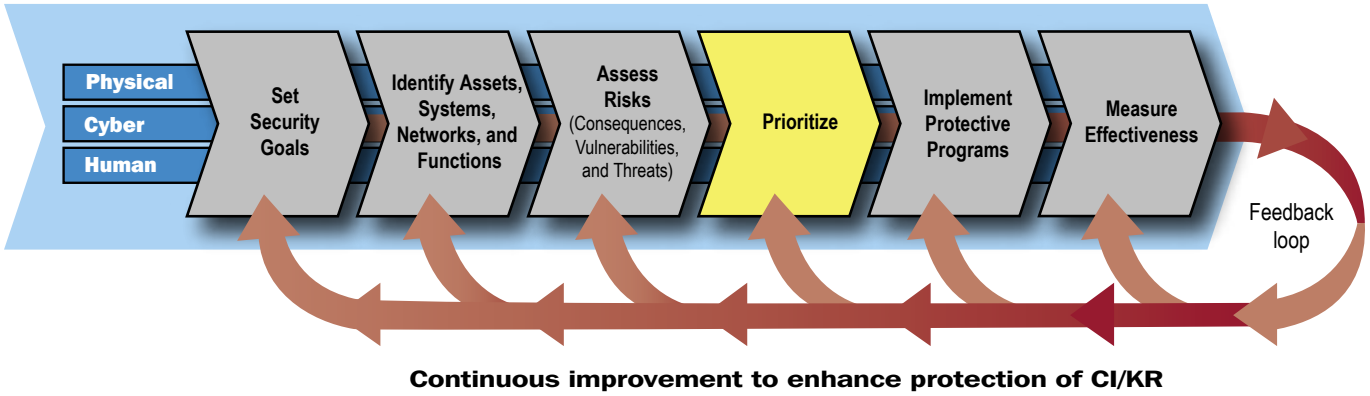
- **Attack-Specific Threat Scenarios:** Attack-Specific Threat Scenarios are detailed vignettes of the specific methods, techniques, and actions terrorists are likely to use to attack specific types of U.S. CI/KR. The scenarios are based on HITRAC analysis of known terrorist capabilities or on their stated intent as derived from intelligence and the study of terrorist tactics, techniques, and capabilities. Threat scenarios are specific enough to be used by corporate or facility-level security officers to support operational security planning.

This product supports facility-level threat surveillance by security forces, owner and operator requests for intelligence information, and risk management action planning. It also provides detailed threat information for the sector-specific threat assessment described below.

- **Sector-Specific Threat Assessment:** DHS uses the information developed for the Terrorist Target Selection Matrix and the Attack-Specific Threat Scenarios to produce Sector-Specific Threat Assessments that provide an overall assessment of the potential terrorist threats posed to each of the CI/KR sectors, as well as an analysis of how these threats relate to sector vulnerabilities and consequences. These assessments include known specific and general terrorist threat information for each sector, as well as relevant background information such as terrorist objectives and motives as they apply to the sector. Each sector-specific report includes the Terrorist Target Selection Matrix for the sector and specifies those Attack-Specific Threat Scenarios that may be relevant to the sector. The assessments are updated on a routine basis to include the most current intelligence findings and operational trends analyses. HITRAC works with each sector to develop and provide threat products that are tailored to meet sector-specific and subsector information needs.

This product is used to support detailed sector-level planning, including SSP development and implementation, and also to provide the detailed threat information necessary for additional security-related planning.

Figure 3-6: NIPP Risk Management Framework: Prioritize



3.4 Prioritize

Prioritization for CI/KR protection is used to focus planning, foster coordination, and support effective resource allocation and incident management, response, and restoration decisions.

The NIPP risk management framework provides the process for developing comparable estimates of the risk relevant to CI/KR. The framework is applicable to risk assessments on an asset, system, network, function, sector, State, regional, or national basis. Comparing the risk faced by different entities helps identify where risk mitigation is most pressing, and to subsequently determine the most cost-effective protective actions, including those related to the cyber and human elements of CI/KR. This identifies which CI/KR should be given priority for protection and which alternative protective actions represent the best investment based on risk. The prioritization process also provides information that can be used during incident response to help inform decisionmakers regarding issues associated with CI/KR restoration.

3.4.1 The Prioritization Process

The prioritization process involves aggregating, combining, and analyzing risk assessment results to determine which assets, systems, networks, functions, sectors, or other relevant groupings face the highest risk. This process leads to a comprehensive picture of risk for the relevant CI/KR groups and allows protection priorities to be established; it also provides the basis for understanding the risk-mitigation benefits that, along with costs, are used to support protection planning and the informed allocation of resources.

This process involves two related activities: The first determines which sectors, regions, or other aggregation of CI/KR assets, systems, networks, or functions are subject to the highest risk as calculated using the NIPP risk management framework. Those exposed to the greatest risk are accorded the highest priority in risk management program development. The second activity determines which protective actions are expected to provide the greatest mitigation of risk for any given investment. The risk management initiatives that result in the greatest risk mitigation for the investment proposed are accorded the highest priority in program design, resource allocation, budgeting, and implementation. This approach ensures that programs make the greatest contribution possible to overall CI/KR risk mitigation in the context of resources available.

Both of these activities involve translating different risks into common and comparable indices that can be combined and synthesized. The specific mathematical approach to this normalization process is described in other, more detailed guidance documents such as the Risk Analysis Methodology Report prepared by DHS each fiscal year to support the homeland security grants program. Although the procedure is based on a mathematical process, it also involves the judgment and assumptions of risk analysts and decisionmakers. These factors significantly shape the process and are clearly stated and documented to ensure that they are understandable to other security partners and the public.

Assessments become more complex at more aggregate levels, as when comparisons are necessary across sectors. Such assessments rely more heavily on the subjective interpretation of estimates derived from the data that can be collected, as well as differences in assumptions.

3.4.2 Tailoring Prioritization Approaches to Sector Needs

CI/KR security partners rely on different approaches to prioritize risk management activities according to specific sector needs, risk landscapes, security approaches, and busi-

ness environment. For example, asset-based priorities may be appropriate for CI/KR that is facility based, or for assets, systems, or networks that can be exploited and used as weapons. Function-based priorities may more effectively ensure continuity of operations in the event of a terrorist attack or natural disaster in sectors where CI/KR resilience may be more important than CI/KR hardening. Programs to protect assets, systems, or networks give priority to investments that protect physical assets or ensure resilience in virtual systems depending on which option best enables CI/KR risk management.

To ensure a consistent approach to risk analysis for CI/KR protection, security partners establish priorities based on risk analysis that is consistent with the NIPP baseline criteria for risk assessment methodologies; these can be quick-response, top-down assessments using surrogate data or data at high levels of CI/KR aggregation (e.g., functions of population density as a surrogate for casualties), or they can be detailed bottom-up analyses using detailed data on specific individual facilities and employing sophisticated threat models.

3.4.3 The Uses of Prioritization

Prioritization based on risk or the individual components of risk is used for different purposes at several points in the risk management process. For example, in the sharing and collection of risk-related data, top-screening methods based on estimated consequences are used to identify the information that is pertinent to assets, systems, networks, and functions that are essential to business or mission continuity.

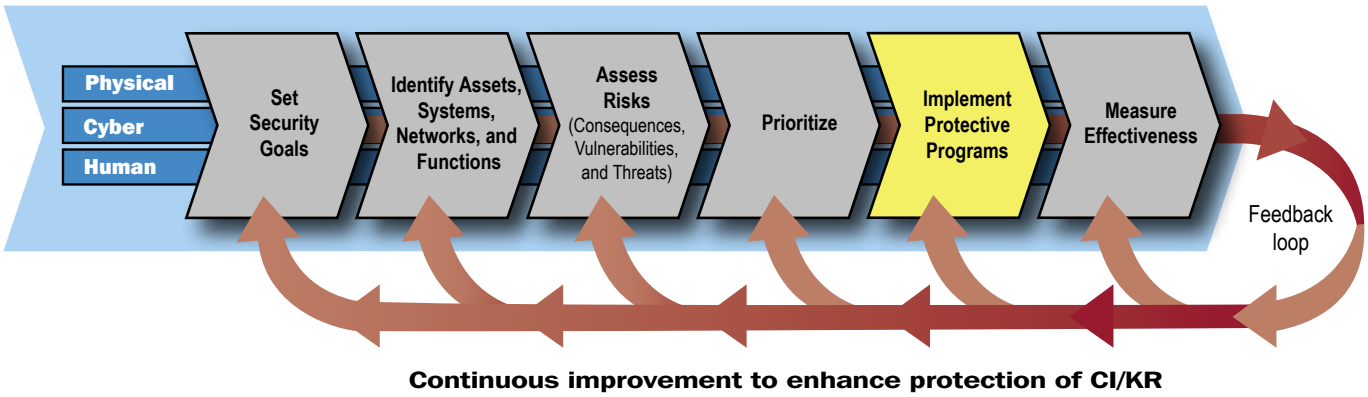
A primary use of prioritization is to inform resource allocation decisions, such as where protection programs should be instituted; the appropriate level of investment in these programs; and which protection measures offer the greatest return on investment. Because resources for CI/KR protection are limited, risk analysis based on empirical information must be completed before sound priorities can be established.

Different possible risk management initiatives involve different degrees of cost and effectiveness. In the design of protection programs and budgets, priority is given to those protective measures that provide the greatest mitigation of risk for the resources that are available. To determine this, security partners designing programs and budgets must evaluate the effect of these different options on reducing or mitigating consequence, vulnerability, or threat. In this process, they combine cost estimates with risk-mitigation estimates in a cost-benefit analysis to choose between the different options, and should consider as wide a range of program options as is practical in making the choice.

At the national level, DHS is responsible for overall national risk-based CI/KR prioritization in close collaboration with the SSAs and other security partners.

The result of the prioritization process is information. This information reflects CI/KR protection and risk-mitigation requirements and provides the rationale and justification for implementing specific programs or actions. Although for some specific purposes, a master inventory of facilities or sites in priority order may be useful, the results of the prioritization process are primarily used in other ways, such as in guidance documents or the decisions underpinning department budget requests. For example, the NADB is not a prioritized list of CI/KR, but rather a database of information on infrastructure assets, systems, and networks that allows analysts to compute risk to help inform decisionmakers in a range of different situations. At the national level, the results of the prioritization process are reflected in a number of guidance documents. These include the Sector CI/KR Protection Annual Reports from the SSAs to the Secretary of Homeland Security and the National CI/KR Protection Annual Report that DHS develops to summarize national CI/KR protection priorities and requirements and to inform the Federal budget process.

Figure 3-7: NIPP Risk Management Framework: Implement Protective Programs



3.5 Implement Protective Programs

The risk assessment and prioritization process enables DHS, SSAs, and other security partners to identify opportunities to enhance current CI/KR protection programs where they will offer the greatest benefit. Security partners give priority in the development of CI/KR protection programs to focus resources on assets, systems, networks, and functions that are deemed to be at the greatest risk.

The risk assessment and prioritization activities within each sector will help identify requirements for current protective programs and shortfalls for future efforts. Some of the identified shortfalls or opportunities for improvement will be filled by owner/operators, either voluntarily or based on various forms of incentives. Other shortfalls will be addressed through the protective programs each sector develops under the SSP or through cross-sector or national initiatives undertaken by DHS.

The Nation's CI/KR is widely distributed in both a physical and logical sense. Effective CI/KR protection requires both distributed implementation of protective programs by security partners, and focused national leadership to ensure implementation of a comprehensive, coordinated, and cost-effective approach that helps to reduce or manage the risks to the Nation's most critical assets, systems, networks, and functions. At the implementation level, protective programs consist of diverse actions undertaken by various security partners. From the leadership perspective, programs are structured to address coordination and cost-effectiveness.

The following sections describe the nature and characteristics of best practice protective programs, as well as some existing programs that could be applied to specific assets, systems, networks, or functions.

3.5.1 Protective Actions

Protective actions involve measures designed to prevent, deter, and mitigate the threat; reduce vulnerability to an attack or other disaster; minimize consequences; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack, natural disaster, or other incident. Protective actions vary across a wide spectrum of activities as follows:

- **Deter:** Cause the potential attacker to perceive that the risk of failure is greater than that which they find acceptable. Examples include improved awareness and security (e.g., restricted access, vehicle checkpoints) and enhanced police and/or security officer presence;
- **Devalue:** Reduce the attacker's incentive by reducing the target's value. Examples include developing redundancies and maintaining backup systems or key personnel;
- **Detect:** Identify potential attacks and validate and/or communicate the information, as appropriate. General detection activities include intelligence gathering, analysis of surveillance activities, and trend analysis of law enforcement reporting. For specific assets, examples include intrusion-detection systems, network monitoring systems, operation alarms, surveillance, detection and reporting, and employee security awareness programs; and
- **Defend:** Protect assets by preventing or delaying the actual attack, or reducing an attack's effect on an asset, system, or network. Examples include perimeter hardening by enhancing buffer zones, fencing, structural integrity, and cyber defense tools such as antivirus software.

Protective programs also may include actions that mitigate the consequences of an attack or incident. These actions are focused on the following aspects of preparedness:

- **Mitigate:** Lessen the potential impacts of an attack, natural disaster, or accident by introducing system redundancy and resiliency, reducing asset dependency, or isolating downstream assets;
- **Respond:** Activities designed to enable rapid reaction and emergency response to an incident, such as conducting exercises and having adequate crisis response plans, training, and equipment; and
- **Recover:** Allow businesses and government organizations to resume operations quickly and efficiently, such as using comprehensive mission and business continuity plans that have been developed through prior planning.

Generally, it is considered more cost-effective to build security into assets, systems, and networks than to retrofit them with security measures after initial development. Accordingly, security partners should consider how risk management, robustness, resiliency, and appropriate physical and cyber security enhancements could be incorporated into the design and construction of new CI/KR.

In situations where robustness and resiliency are keys to CI/KR protection, providing protection at the system level rather than at the individual asset level may be more effective and efficient (e.g., if there are many similar facilities, it may be easier to allow other facilities to provide the infrastructure service rather than to protect each facility). Both are possible approaches to meeting NIPP objectives.

3.5.2 Characteristics of Effective Protective Programs

Characteristics of effective CI/KR protective programs include, but are not limited to, the following:

- **Comprehensive:** Effective protective programs must address the physical, cyber, and human elements of CI/KR, as appropriate, and consider long-term, short-term, and sustainable activities. SSPs describe programs and initiatives to protect CI/KR within the sector (e.g., operational changes, physical protection, equipment hardening, cyber protection, system resiliency, backup communications, training, response plans, and security system upgrades).
- **Coordinated:** Because of the highly distributed and complex nature of the various CI/KR sectors, the responsibility for protecting CI/KR must be coordinated:
  - CI/KR owners and operators (public or private sector) are responsible for protecting property, information, and people through measures that manage risk to help ensure more resilient operations and more effective loss prevention. These measures include increased awareness of terrorist threats and implementation of operational responses to reduce vulnerability (e.g., changing daily routines, keeping computer software and virus-checking applications up to date, and applying fixes for known software defects).
  - State, local, and tribal authorities are responsible for providing or augmenting protective actions for assets, systems, and networks that are critical to the public within their jurisdiction and authority. They develop protective programs, supplement Federal guidance and expertise, implement relevant Federal programs (such as the Urban Area Security Initiative or the Buffer Zone Protection Program (BZPP)), and provide specific law enforcement capability as needed. When appropriate, they have access to Federal resources to meet jurisdictional protection priorities.
  - Federal agencies are responsible for enabling or augmenting protection for CI/KR that is nationally critical or coordinating the efforts of security partners and the use of resources from different funding sources. DHS, SSAs, and other Federal departments and agencies carry out these responsibilities while respecting the authorities of State, local, and tribal governments, and the prerogatives of the private sector.
  - SSAs, in conjunction with security partners, provide information on the most effective long-term protective strategies, develop protective programs, and coordinate the implementation of programs for their sectors. For some sectors, this includes the development and sharing of best practices and related criteria, guidance documents, and tools.
  - DHS, in collaboration with SSAs and other public and private sector partners, serves as the national focal point for the development, implementation, and coordination of protective programs (including cyber security efforts) for those assets that are deemed nationally critical.
- **Cost-Effective:** Effective CI/KR protective programs seek to use resources efficiently by focusing on actions that offer the greatest mitigation of risk for any given expenditure. The following is a discussion of factors that should be considered when assessing the cost-effectiveness and public benefits derived through implementation of CI/KR protection initiatives:
  - **Operating with full information and lowering coordination costs:** The NIPP describes the mechanisms that enable the use of information regarding threats and corresponding protective actions. It includes information sharing among security partners; provision of a dedicated communications network; and the use of established, interoperable industry and trade association communications mechanisms. The NIPP also helps to lower the cost of coordination through such mechanisms as security partnership arrangements and, where appropriate, the use of a regulatory or incentives-based framework to encourage or drive action.
  - **Addressing the present-future tradeoff in long lead-time investments:** The NIPP provides the processes and coordinating structures that allow State, local, and tribal governments and private sector partners to effectively use long lead-time approaches to CI/KR protection.
  - **Providing for appropriate roles among security partners:** Appropriate roles for CI/KR protection reflect basic responsibilities and shared risks and burdens. CI/KR owners and operators are responsible for protecting property, information, and people through measures that manage risk and help ensure more resilient operations and more effective loss prevention. State, local, and tribal authorities are responsible for providing or augmenting protective actions for assets, systems, and networks that are critical to the public within their jurisdiction and authority. Federal agencies are responsible for coordinating and enabling protection for CI/KR that is nationally critical. They coordinate with regulatory agencies to help

ensure that CI/KR protection issues are fully understood and considered in their deliberations. As discussed in chapter 7, they may make Federal resources available for selected State, local, or tribal CI/KR protection efforts through grant programs in certain circumstances.

  - **Matching the underlying economic incentives of each security partner to the extent possible:** The NIPP supports market-based economic incentives wherever possible by relying on security partners to undertake those efforts that are in their own interest and complementing those efforts with additional resources where necessary and appropriate. This coordinated approach builds on efforts that have proven to be effective and that are consistent with best business practices, such as owners and operators selecting the measures that are best suited to their particular risk profile and needs.

  - **Addressing the public-interest aspects associated with CI/KR protection:** Protective actions for CI/KR that provide benefits to the public at large go beyond the actions that benefit owners and operators, or even those that benefit the public residing in a particular State, region, or locality. Such additional actions reflect different levels of the public interest—some CI/KR are critical to the national economy and to national well-being; some CI/KR are critical to a State, region, or locality; some CI/KR are critical only to the individual owner/operator or direct customer base. Actions to protect the public's interest that require investment beyond the level that those directly responsible for protection are willing and able to provide must be of sufficient priority to warrant the use of the limited resources that can be provided from public funding or may require regulatory action or appropriate incentives to encourage the private sector to undertake them.

- **Risk-Based:** Protective programs focus on mitigating risk. Protective actions should be designed to allow measurement, evaluation, and feedback based on risk mitigation. This allows owners, operators, and SSAs to reevaluate risk after the program has been implemented. Protective programs use different mechanisms for addressing each element of risk and combine their effects to achieve overall risk mitigation. These mechanisms include:

  - **Consequences:** Protective programs directly limit or manage consequences by reducing the possible loss resulting from a terrorist attack or other disaster through redundant system design, backup systems, and alternative sources for raw materials or information.

  - **Vulnerability:** Protective programs directly reduce vulnerability by decreasing the susceptibility to destruction, incapacitation, or exploitation by correcting flaws or strengthening weaknesses in assets, systems, and networks.

  - **Threat:** Protective programs indirectly reduce threat by making assets, systems, or networks less attractive targets to terrorists by lessening vulnerability and lowering consequences. As a result, terrorists are less likely to achieve their objectives and, therefore, less likely to focus on the CI/KR in question.

3.5.3 Protective Programs, Initiatives, and Reports

DHS, in collaboration with SSAs and other security partners, undertakes a number of protective programs, initiatives, activities, and reports that support CI/KR protection. Many of these are available to or provide resources for security partners. These activities span a wide range of efforts that include, but are not limited to, the following:

- **Buffer Zone Protection Program:** A grant program designed to provide resources to State and local law enforcement to enhance the protection of a given critical facility.

- **Assistance Visits:** Facility security assessments jointly conducted by a federally led team and facility owners and operators that are designed to facilitate vulnerability identification and mitigation discussions between security partners and individual owners and operators.

- **Training Programs:** Training programs are designed to provide security partners a source from which they can obtain specialized training to enhance CI/KR protection. Subject matter, course length, and location of training can be tailored to security partner needs.

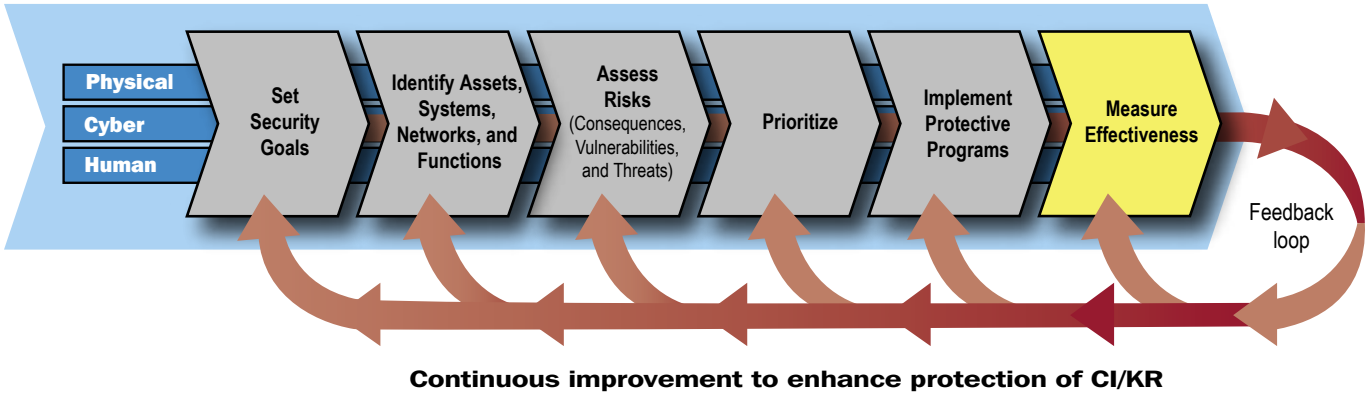
- **Control Systems Security:** DHS coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CI/KR sectors.

A detailed discussion of DHS-supported programs is provided in appendix 3B.

SSAs and other Federal departments and agencies also oversee protective programs, initiatives, and activities that support CI/KR protection. Many of these are also available or provide resources for security partners. Examples include:

- The Department of Veterans Affairs created a methodology also used by the Smithsonian Institution and adapted by

Figure 3-8: NIPP Risk Management Framework: Measure Effectiveness



Federal Emergency Management Agency (FEMA) Manual 452, *Risk Management: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, to assess the risk to and mitigation for hundreds of buildings and museums.

- DOT manages a Pipeline Safety grant program that supports efforts to develop and maintain State natural gas, liquefied natural gas, and hazardous liquid pipeline safety programs.
- HHS is conducting pilot tests that include a tribal hospital, a local substance abuse treatment center, and an owner/operator administrative office in preparation for a vulnerability assessment of more than 4,000 health care-related facilities.

Other protective activities include developing and providing informational reports, such as the DHS Characteristics of Common Vulnerabilities Reports and the Indicators of Terrorist Activity Reports, which are available to all State and Territorial homeland security offices. In addition to threat and vulnerability information, informational reports also include best practices for protection measures. One report in particular, FEMA's Risk Management Series, addresses the protection of buildings and is applicable across sectors.

3.6 Measure Effectiveness

Measuring effectiveness drives continuous improvement of CI/KR risk-mitigation programs at the sector level and overall program performance at the national level. The NIPP uses a metrics-based system to provide feedback on efforts to attain the goal and supporting objectives articulated in chapter 1. The metrics also provide a basis for establishing accountability, documenting actual performance, facilitating diagnoses, promoting effective management, and reassessing goals and objectives. Metrics offer a quantitative assessment to affirm that specific objectives are being met or to articulate gaps in the national effort or supporting sector efforts. They enable identification of corrective actions and provide decisionmakers with a feedback mechanism to help them make appropriate adjustments. They can also provide qualitative insights to help make informed decisions. Cost-benefit analyses of programs, lessons learned from exercises, actual incidents, and alerts provide additional objective input into the process.

3.6.1 NIPP Metrics and Measures

3.6.1.1 Measuring Performance

The NIPP risk management framework uses three types of quantitative indicators to measure program performance, to include cost-effectiveness. These indicators span a wide range: descriptive measures are usually the easiest and least costly to collect, but bear only an indirect relationship to the actual performance of CI/KR protection efforts; outcome measures most directly measure performance, but often have limitations due to the need for modeling, assumptions, or complex formulas in calculating them. The NIPP risk management framework relies on a mix of these measures that will change over time as the framework matures and as security partners learn which measures are the most useful in actual practice:

- **Descriptive Measures** are used to understand sector resources and activities; they do not reflect CI/KR protection performance. Examples include the number of facilities in a jurisdiction; the population resident or working within typical incident effects footprints; and the number, nature, and location of suppliers in an infrastructure service provider's supply chain.

- **Process (or Output) Measures** are used to measure whether specific activities were performed as planned, tracking the progression of a task, or reporting on the output of a process such as inventorying assets. Process measures show progress toward performing the activities necessary to achieve CI/KR protection goals. They also help build a comprehensive picture of CI/KR protection status and activities. Examples include the number of protective programs implemented in a specific fiscal year and the level of investment for each, the number of detection systems installed at facilities in a given sector, the proportion of a facility's workforce that has completed training, and the level of response to a data call for asset information.
- **Outcome Measures** track progress toward a strategic goal by beneficial results rather than level of activity. As the NIPP is implemented, process measures will be deemphasized in favor of outcome measures. Examples include the reduction of risk measured by comparing 1 year of comparative analysis for a specific sector to another, and the overall risk mitigation achieved nationally by a particular CI/KR protection initiative.

3.6.1.2 Core Metrics and Sector-Specific Metrics

Quantitative indicators are used for two different groups of metrics to support national assessments: (1) core metrics, which apply to all sectors; and (2) sector-specific metrics, which are appropriate only for an individual sector.

Core Metrics are common across all sectors and represent a set of descriptive, process, and outcome data that enable measurement of progress in SSP implementation. Examples include the number of assets, systems, and networks with a potential for medium or high consequence, and the number of assets, systems, and networks with completed vulnerability analyses. Core metrics are basic measures that can be tracked across each sector to enable comparison and analysis between different types of CI/KR. Resources are allocated to those activities that best accomplish CI/KR risk-mitigation goals. Activities that do not advance these goals will be redesigned or eliminated over time.

Core metrics are consistent with the National Preparedness Goal and its supporting Universal Task List (UTL) and Target Capabilities List (TCL). DHS will specify an initial set of core metrics and work with SSAs and other security partners to refine them as experience in their use is gained over time.

Sector-Specific Metrics are tailored to the unique characteristics of each sector and are used to assist in monitoring progress within a specific sector. Sector-specific metrics and the means of monitoring progress against those metrics are developed in a collaborative process that includes DHS, the SSAs, and other public and private sector security partners, as appropriate. For example, sector-specific metrics might include the percentage of shipments moving through a specific port that is subjected to detailed screening or improvements in the time required to obtain results from test samples.

3.6.2 Gathering Performance Information

DHS works with the SSAs and sector security partners to gather the information necessary to measure the level of performance associated with each set of core and sector-specific metrics. Given the inherent differences in CI/KR sectors, a one-size-fits-all approach to gathering this information is not appropriate. DHS also works with SSAs and sector security partners to determine the appropriate measurement approach to be included in the sector's SSP and to help ensure that security partners engaged with multiple sectors or in cross-sector matters are not subject to unnecessary redundancy or conflicting guidance in information collection. Information collected as part of this effort is protected as discussed in detail in chapter 4.

SSAs identify and, as appropriate, share or facilitate the sharing of best practices based on the effective use of metrics to improve program performance.

3.6.3 Assessing Performance and Reporting on Progress

HSPD-7 requires each SSA to provide the Secretary of Homeland Security with an annual report on their efforts to identify, prioritize, and coordinate the protection of CI/KR in their respective sectors. The report from each SSA will be sent to DHS annually. The reports are due no later than July 1 of each year.

The Sector CI/KR Annual Protection Reports provide the following information:

- Provide a common vehicle across all CI/KR sectors for communicating CI/KR protection performance and progress to security partners and other government entities;
- Establish a baseline of existing sector-specific CI/KR protection priorities, programs, and initiatives against which future improvements will be assessed;
- Identify sector priorities and out-year requirements with a focus on projected shortfalls in resources for sector-specific CI/KR protection and for protection of CI/KR within the sector that is deemed to be critical at the national level;

- Determine and explain how sector efforts support the national effort;
- Provide an overall progress report for the CI/KR sector and measure that progress against the CI/KR protection goals and objectives for that sector as described in the SSP;
- Provide feedback to DHS, the CI/KR sectors, and other government entities to provide the basis for the continuous improvement of the CI/KR protection program; and
- Help identify best practices from successful programs and share these within and among sectors.

SSAs work in close collaboration with sector security partners, the respective SCCs and the GCCs, and other organizations in developing this report. DHS works with SSAs to assess progress made toward goals in each sector based on these reports.

DHS compiles the sector reports into a national cross-sector report that describes overall progress toward CI/KR protection goals on a national basis and makes recommendations to the Executive Office of the President for prioritized resource allocation across the Federal Government to meet national CI/KR protection requirements. A more detailed discussion of the national resource allocation process for CI/KR protection is included in chapter 7.

In addition to these annual reports, SSAs regularly update their measurements of CI/KR status and protection levels to support DHS status tracking and comprehensive inventory update. By maintaining a regularly updated knowledge base, DHS is able to quickly compile real-time CI/KR status and protection posture to respond to changing circumstances as indicated by tactical intelligence assessments of terrorist threats or natural disaster damage assessments. This helps inform resource allocation decisions during incident response and other critical operations supporting the homeland security mission.

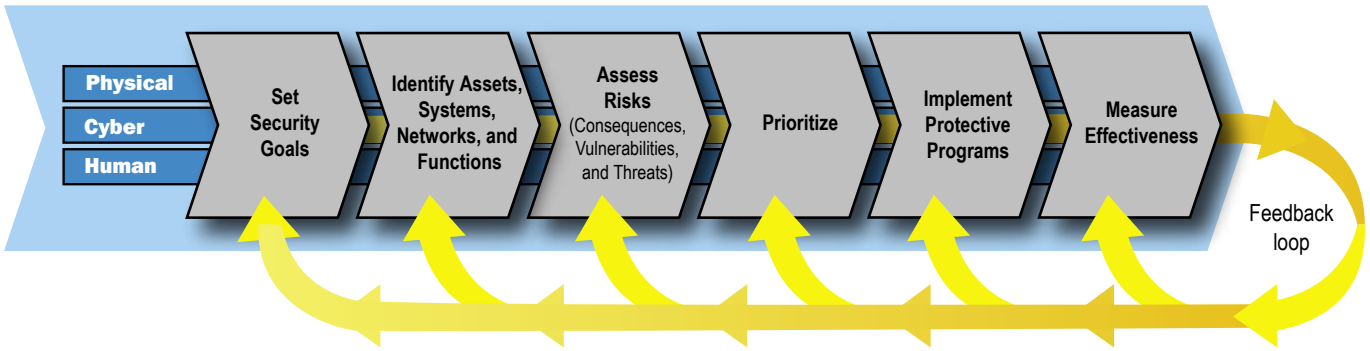
3.7 Using Metrics and Performance Measurement for Continuous Improvement

By using NIPP metrics to compare performance to goals, security partners adjust and adapt the Nation's CI/KR protection approach to account for progress achieved, as well as for changes in the threat and other relevant environments. At the national level, NIPP metrics are used to focus Federal and security partner attention on areas of CI/KR protection that warrant additional resources or other changes. If a comparison of performance against goals using NIPP metrics reveals that there is insufficient progress (e.g., information-sharing mechanisms have not been established and risk assessments have not been conducted, or one or more sectors have a significant portion of their assets rated as high risk), DHS and its security partners will undertake actions to focus efforts on addressing those particular areas of concern.

Information gathered in support of the risk management framework process helps determine adjustments to specific CI/KR protection activities. For instance, as protective programs are implemented, the consequences and vulnerabilities associated with the asset, system, network, or function change. Accordingly, the national risk profile is reviewed routinely to help inform current and prospective allocation of resources in light of recently implemented protective actions or other factors, such as increased understanding of potential system-wide cascading consequences, new threat intelligence, etc.

In addition to quantitative measures, the NIPP provides mechanisms for qualitative feedback that can be applied to augment and improve the effectiveness and efficiency of public and private sector CI/KR protective programs. DHS works with security partners to identify and share lessons learned and best practices for all aspects of the risk management process. DHS also works with SSAs to share relevant input from security partners and other sources that can be used as part of the national effort to continuously improve CI/KR protection.

Figure 3-9: NIPP Risk Management Framework: Feedback Loop for Continuous Improvement of CI/KR Protection



4. Organizing and Partnering for CI/KR Protection

The enormity and complexity of the Nation's CI/KR, the distributed character of its associated protective architecture, and the uncertain nature of the terrorist threat and manmade or natural disasters make the effective implementation of protection efforts a great challenge. To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives described in chapter 1. DHS, in close collaboration with the SSAs, is responsible for overall coordination of the NIPP partnership organization and information-sharing network.

4.1 Leadership and Coordination Mechanisms

The coordination mechanisms described below establish linkages among CI/KR protection efforts at the Federal, State, regional, local, tribal, and international levels, as well as between public and private sector security partners. In addition to direct coordination between security partners, the structures described below provide a national framework that fosters relationships and facilitates coordination within and across CI/KR sectors:

- **National-Level Coordination:** The DHS Office of Infrastructure Protection (OIP) facilitates overall development of the NIPP and SSPs, provides overarching guidance, and monitors the full range of associated coordination activities and performance metrics.
- **Sector Partnership Coordination:** The Private Sector Cross-Sector Council (i.e., the Partnership for Critical Infrastructure Security (PCIS)), the Government Cross-Sector Council (made up of two subcouncils: the NIPP Federal Senior Leadership Council (FSLC) and the State, Local, and Tribal Government Coordinating Council (SLTGCC)), and individual SCCs and GCCs create a structure through which representative groups from Federal, State, local, and tribal governments and the private sector can collaborate and develop consensus approaches to CI/KR protection.
- **Regional Coordination:** Regional partnerships, groupings, and governance bodies enable CI/KR protection coordination among security partners within and across geographical areas and sectors. Such bodies are composed of representatives from industry and State, local, and tribal entities located in whole or in part within the planning area for an aggregation of high-risk targets, urban areas, or cross-sector groupings. They facilitate enhanced coordination between jurisdictions within a State where CI/KR cross multiple jurisdictions, and help sectors coordinate with multiple States that rely on a common set of CI/KR. They also are organized to address common approaches to a wide variety of natural or manmade hazards.
- **International Coordination:** The United States-Canada-Mexico Security and Prosperity Partnership; the North Atlantic Treaty Organization's (NATO's) Senior Civil Emergency Planning Committee; certain government councils, such as the Committee on Foreign Investment in

the United States (CFIUS); and consensus-based nongovernmental or public-private organizations, such as the global Forum of Incident Response and Security Teams (FIRST), enable a range of CI/KR protection coordination activities associated with established international agreements.

4.1.1 National-Level Coordination

DHS, in collaboration with the SSAs, oversees the coordination and integration of national-level CI/KR protection activities through the DHS/OIP. In support of security partner coordination, DHS:

- Leads, integrates, and coordinates the execution of the NIPP, in part by acting as a central clearinghouse for the information-sharing and coordination activities of the individual sector governance structures;
- Facilitates the development and ongoing support of these security partner governance and coordination structures or models;
- Facilitates NIPP revisions and updates using a comprehensive national review process;
- Ensures that effective policies, approaches, guidelines, and methodologies regarding partner coordination are developed and disseminated to enable SSAs and other security partners to carry out NIPP responsibilities;
- Facilitates the sharing of CI/KR protection-related best practices and lessons learned;
- Facilitates security partner participation in preparedness activities, planning, readiness exercises, and public awareness efforts; and
- Ensures cross-sector coordination of SSPs to avoid duplicative requirements and reporting, and conflicting guidance.

4.1.2 Sector Partnership Coordination

The goal of these organizational structures, partnerships, and information-sharing networks is to establish the context, framework, and support for activities required to implement and sustain the national CI/KR protection effort. DHS will issue coordinated guidance on the framework for CI/KR public-private partnerships, as well as metrics to measure their effectiveness.

The NIPP relies on the sector partnership model, illustrated in figure 4-1, as the primary organizational structure for coordinating CI/KR efforts and activities. The sector partnership model encourages formation of SCCs and GCCs as described below. DHS also provides guidance, tools, and support to enable these groups to work together to carry out their respective roles and responsibilities. SCCs and corresponding GCCs work in tandem to create a coordinated national framework for CI/KR protection within and across sectors.

4.1.2.1 Private Sector Cross-Sector Council

Cross-sector issues and interdependencies between the SCCs will be addressed through a Private Sector Cross-Sector Council (i.e., the PCIS):

- **Partnership for Critical Infrastructure Security:** The PCIS membership is comprised of one or more members and their alternates from each of the SCCs. The partnership coordinates cross-sector initiatives to support CI/KR protection by identifying legislative issues that affect such initiatives and by raising awareness of issues in CI/KR protection. The primary activities of the PCIS include:
  - Providing senior-level, cross-sector strategic coordination through partnership with DHS and the SSAs;
  - Identifying and disseminating CI/KR protection best practices across the sectors;
  - Participating in coordinated planning efforts related to the development, implementation, and revision of the NIPP Base Plan and SSPs; and
  - Coordinating with DHS to support efforts to plan and execute the Nation's CI/KR protection mission.

4.1.2.2 Government Cross-Sector Council

Cross-sector issues and interdependencies between the GCCs will be addressed through the Government Cross-Sector Council, which is comprised of two subcouncils: the NIPP FSLC and the SLTGCC:

- **NIPP Federal Senior Leadership Council:** The objective of the NIPP FSLC is to drive enhanced communications and coordination between and among Federal departments and agencies with a role in implementing the NIPP and HSPD-7. The Council's primary activities include:
  - Forging consensus on CI/KR risk management strategies;
  - Evaluating and promoting implementation of risk management-based CI/KR protection programs;
  - Advancing CI/KR protection collaboration within and across sectors;
  - Advancing CI/KR protection collaboration with the international community; and

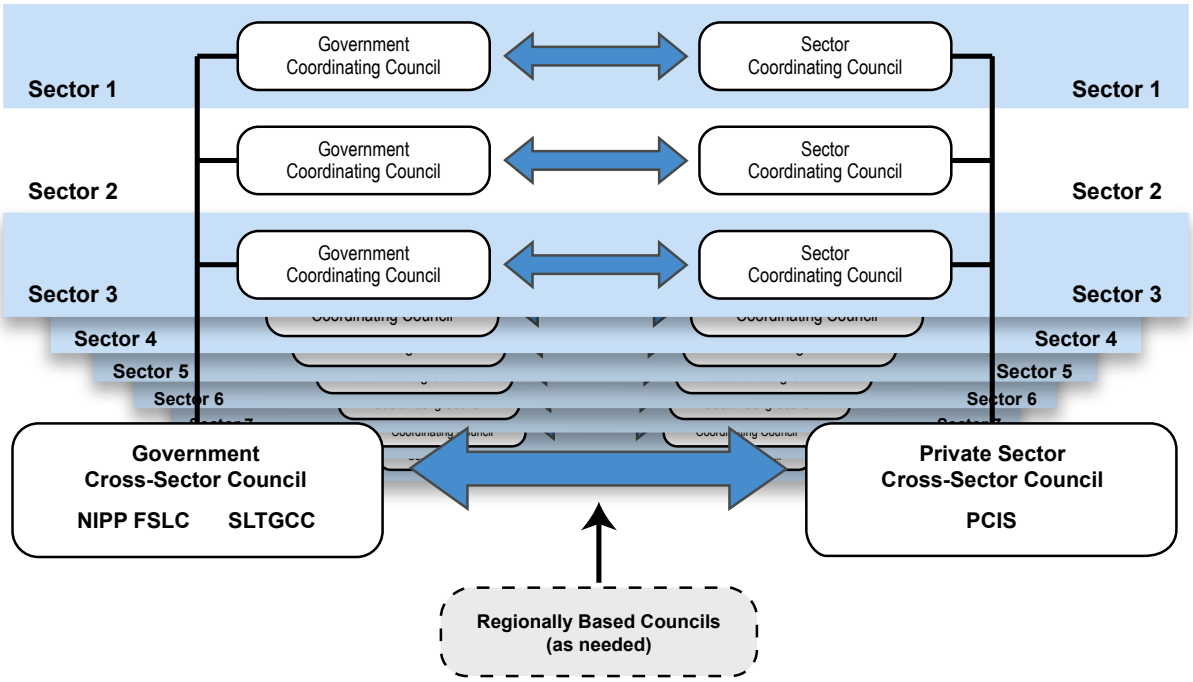
– Evaluating and reporting on the progress of Federal CI/KR protection activities.

- **State, Local, and Tribal Government Coordinating Council:** The SLTGCC serves as a forum to ensure that State, local, and tribal homeland security advisors or their designated representatives are fully integrated as active participants in national CI/KR protection efforts and to provide an organizational structure to coordinate across jurisdictions on State- and local-level CI/KR protection guidance, strategies, and programs. The SLTGCC will provide the State, local, or tribal perspective or feedback on a wide variety of CI/KR issues. The primary functions of the SLTGCC include the following:
  - Providing senior-level, cross-jurisdictional strategic communications and coordination through partnership with DHS, the SSAs, and private sector owners and operators;
  - Participating in planning efforts related to the development, implementation, update, and revision of the NIPP Base Plan and SSPs;
  - Coordinating strategic issues and issue management resolution among State, local, and tribal security partners;
  - Coordinating with DHS to support efforts to plan, implement, and execute the Nation's CI/KR protection mission; and
  - Providing DHS with information on State-, local-, and tribal-level CI/KR protection initiatives; activities; and best practices.

The cross-sector bodies described in sections 4.1.2.1 and 4.1.2.2 will convene in joint session and/or working groups, as appropriate, to address cross-cutting CI/KR protection issues. The NIPP-related functions of the cross-sector bodies include activities to:

- Provide or facilitate coordination, communications, and strategic-level information sharing across sectors and between and among DHS, the SSAs, supporting Federal departments and agencies, and other public and private sector security partners;
- Identify issues shared by multiple sectors that would benefit from common investigations and/or solutions;
- Identify and promote best practices from individual sectors that have applicability to other sectors;
- Contribute to cross-sector planning and prioritization efforts, as appropriate; and
- Provide input to the government on R&D efforts that would benefit multiple sectors.

Figure 4-1: Sector Partnership Model



4.1.2.3 Sector Coordinating Councils

The sector partnership model encourages CI/KR owners and operators to create or identify an SCC as the principal entity for coordinating with the government on a wide range of CI/KR protection activities and issues. SCCs should be self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership. Specific membership will vary from sector to sector, reflecting the unique composition of each sector; however, membership should be representative of a broad base of owners, operators, associations, and other entities—both large and small—within a sector.

The SCCs enable owners and operators to interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal sector policy coordination and planning entities. Sectors also rely on ISACs, or other information-sharing mechanisms, which provide operational and tactical capabilities for information sharing and, in some cases, support for incident response activities. (A more detailed discussion of ISAC roles and responsibilities is included in section 4.2.7.)

The primary functions of an SCC include the following:

- Represent a primary point of entry for government into the sector for addressing the entire range of CI/KR protection activities and issues for that sector;
- Serve as a strategic communications and coordination mechanism between CI/KR owners, operators, and suppliers, and with the government during response and recovery as determined by the sector;
- Identify, implement, and support the information-sharing capabilities and mechanisms that are most appropriate for the sector. ISACs may perform this role if so designated by the SCC;
- Facilitate inclusive organization and coordination of the sector's policy development regarding CI/KR protection planning and preparedness, exercises and training, public awareness, and associated plan implementation activities and requirements;
- Advise on integration of Federal, State, regional, and local planning with private sector initiatives; and
- Provide input to the government on sector R&D efforts and requirements.

SCCs are encouraged to participate in voluntary consensus standards development efforts to ensure that sector perspectives are included in standards that affect CI/KR protection.[20]

4.1.2.4 Government Coordinating Councils

A GCC is formed as the government counterpart for each SCC to enable interagency and cross-jurisdictional coordination. The GCC is comprised of representatives across various levels of government (Federal, State, local, or tribal) as appropriate to the security landscape of each individual sector. Each GCC is chaired by a representative from the designated SSA with responsibility for ensuring appropriate representation on the GCC and providing cross-sector coordination with State, local, and tribal governments. Each GCC is co-chaired by the DHS Assistant Secretary for Infrastructure Protection or his/her designee.

The GCC coordinates strategies, activities, policy, and communications across government entities within each sector. The primary functions of a GCC include the following:

- Provide interagency strategic communications and coordination at the sector level through partnership with DHS, the SSA, and other supporting Federal departments and agencies;
- Participate in planning efforts related to the development, implementation, update, and revision of the NIPP Base Plan and SSPs;
- Coordinate strategic communications, and issue management and resolution among government entities within the sector; and
- Coordinate with and support the efforts of the SCC to plan, implement, and execute the Nation's CI/KR protection mission.

4.1.2.5 Critical Infrastructure Partnership Advisory Council

The CIPAC directly supports the sector partnership model by providing a legal framework for members of the SCCs and GCCs to engage in joint CI/KR protection-related activities. The CIPAC serves as a forum for government and private sector security partners to engage in a broad spectrum of activities, such as:

- Planning, coordination, implementation, and operational issues;

[20] Voluntary consensus standards are developed or adopted by voluntary consensus standards bodies, both domestic and international. These organizations plan, develop, establish, or coordinate standards through an agreed-upon procedure that relies on consensus, though not necessarily on unanimity. Federal law encourages Federal participation in these bodies to increase the likelihood that standards meet both public and private sector needs. Examples of other standards that are distinct from voluntary consensus standards include non-consensus standards, industry standards, company standards, or de facto standards developed in the private sector but not in the full consensus process, government-unique standards developed by government for its own uses, and standards mandated by law.

- Implementation of security programs;
- Operational activities related to CI/KR protection, including incident response, recovery, and reconstitution; and
- Development and support of national plans, including the NIPP and the SSPs.

The CIPAC membership consists of private sector CI/KR owners and operators, or their representative trade or equivalent associations, from the respective sector's recognized SCC; and representatives of Federal, State, local, and tribal government entities (including their representative trade or equivalent associations) that comprise the corresponding GCC for each sector. DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a FACA-exempt body, pursuant to section 871 of the Homeland Security Act.

4.1.3 Regional Coordination and the Partnership Model

Regional partnerships, organizations, and governance bodies enable CI/KR protection coordination among security partners within and across certain geographical areas, as well as planning and program implementation aimed at a common hazard or threat environment. These groupings include public-private partnerships that cross jurisdictional, sector, and international boundaries and take into account dependencies and interdependencies. They are typically self-organizing and self-governing.

Regional organizations, whether interstate or intrastate, vary widely in terms of mission, composition, and functionality. Regardless of the variations, these organizations provide structures at the strategic and/or operational levels that help to address cross-sector CI/KR planning and protection program implementation. They may also provide enhanced coordination between jurisdictions within a State where CI/KR cross multiple jurisdictions and help sectors coordinate with multiple States that rely on a common set of CI/KR. In many instances, State homeland security advisors serve as focal points for regional initiatives and provide linkages between the regional organizations and the sector partnership model. Based on the nature or focus of the regional initiative, these organizations may link into the sector partnership model, as appropriate, through individual SCCs or GCCs or cross-sector councils. Additionally, DHS may selectively convene regionally based councils to address issues that cross sectors or jurisdictions, as required.

4.1.4 International CI/KR Protection Cooperation

Many CI/KR assets, systems, and networks, both physical and cyber, are interconnected with a global infrastructure that has evolved to support modern economies. Each of the CI/KR sectors is linked in varying degrees to global energy, transportation, telecommunications, cyber, and other infrastructure. This global system creates benefits and efficiencies, but also brings interdependencies, vulnerabilities, and challenges in the context of CI/KR protection. The Nation's safety, security, prosperity, and way of life depend on these "systems of systems," which must be protected both at home and abroad.

The NIPP strategy for international CI/KR protection coordination and cooperation is focused on:

- Instituting effective cooperation with international security partners, as well as high-priority cross-border protective programs. Specific protective actions are developed through the sector planning process and specified in SSPs;
- Implementing current agreements that affect CI/KR protection; and
- Addressing cross-sector and global issues such as cyber security and foreign investment.

International CI/KR protection activities require coordination with the Department of State and must be designed and implemented to benefit the United States and its international security partners.

4.1.4.1 Cooperation With International Security Partners

DHS, in coordination with the Department of State, works with international partners and other entities involved in the international aspects of CI/KR protection to exchange experiences, share information, and develop a cooperative environment to materially improve U.S. CI/KR protection. DHS, the Department of State, and the SSAs work with foreign governments to identify international interdependencies, vulnerabilities, and risk-mitigation strategies, and through international organizations, such as the Group of Eight (G8), NATO, the European Union, the Organization of American States (OAS), and the Organisation for Economic Co-operation and Development (OECD), to enhance CI/KR protection.

While SSAs and owners and operators are responsible for developing CI/KR protection programs to address risks that arise from or include international sources or considerations, DHS manages specific programs to enhance the cooperation and coordination needed to address the unique challenges and opportunities posed by the international aspects of CI/KR protection:

- **International Outreach Program:** DHS, in cooperation with the Department of State and other Federal agencies, carries out international outreach activities to engage foreign governments and international/multinational organizations to promote a global culture of physical and cyber security. These outreach activities enable international cooperation and engage constituencies that often do not traditionally address CI/KR protection. This outreach encourages the development and adoption of best practices, training, and other programs designed to improve the protection of U.S. CI/KR overseas, as well as the reliability of international CI/KR on which this country depends. Other Federal, State, local, tribal, and private sector entities also engage in international outreach that may be related to CI/KR risk mitigation in situations where they work directly with their foreign counterparts.
- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to practice and evaluate the steady-state protection plans and programs put in place by the NIPP. This exercise program engages international partners to address cooperation and cross-border issues, including those related to CI/KR protection. DHS and other security partners also participate in exercises sponsored by international partners.
- **National Cyber Exercises:** DHS and its security partners conduct exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, regional, local, tribal, and international government elements, as well as private sector corporations and coordinating councils.

4.1.4.2 Implementing Current Agreements

Existing agreements with international security partners include bilateral and multilateral partnerships that have been entered into with the assistance of the Department of State. The key partners involved in existing agreements include:

- **Canada and Mexico:** CI/KR interconnectivity between the United States and its immediate neighbors makes the borders virtually transparent. Electricity, natural gas, oil, roads, rail, food, water, minerals, and finished products cross our borders with Canada and Mexico as a routine component of commerce and infrastructure operations. The importance of this trade, and the infrastructures that support it, was highlighted after the terrorist attacks of September 11, 2001, nearly closed both borders. The United States entered into the 2001 Smart Border Declaration with Canada and the 2002 Border Partnership Declaration with Mexico, in part, to address bilateral CI/KR issues. In addition, the 2005 Security and Prosperity Partnership of North America (SPP) established a common approach to security to protect North America from external threats, prevent and respond to threats, and further streamline the secure and efficient movement of legitimate, low-risk traffic across the shared borders.
- **United Kingdom:** DHS has formed a Joint Contact Group (JCG) with the United Kingdom that brings officials into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.
- **Group of Eight**: The G8 underscored its determination to combat all forms of terrorism and to strengthen international cooperation when heads of government attending the July 2005 meeting in Scotland issued a Statement on Counter-Terrorism, citing three areas of focus related to CI/KR protection:
  - To improve the sharing of information on the movement of terrorists across international borders;
  - To assess and address the threat to the transportation infrastructure; and
  - To promote best practices for rail and metro security.
- **North Atlantic Treaty Organization:** NATO addresses CI/KR protection issues through the Senior Civil Emergency Planning Committee, the senior policy and advisory body to the North Atlantic Council on civil emergency planning and disaster relief matters. The committee is responsible for policy direction and coordination of planning boards and committees in the NATO environment. It has developed considerable expertise that applies to CI/KR protection and has planning boards and committees covering ocean shipping, inland surface transport, civil aviation, food and agriculture, industrial preparedness, civil communications planning, civil protection, and civil-military medical issues.

4.1.4.3 Approach to International Cyber Security

The United States proactively integrates its intelligence capabilities to protect the country from cyber attack; its diplomatic outreach, advocacy, and operational capabilities to build awareness, preparedness, capacity, and partnerships in the global community; and its law enforcement capabilities to combat cyber crime wherever it originates. The private sector, international industry associations, and companies with global interests and operations also are engaged to

address cyber security internationally. For example, the U.S.-based Information Technology Association of America participates in international cyber security conferences and forums, such as the India-based National Association for Software and Service Companies Joint Conference. These efforts require interaction between policy and operations functions to coordinate national and international activity that is mutually supportive across the globe:

- **International Cyber Security Outreach:** DHS, in cooperation with the Department of State, other Federal departments and agencies and the private sector, engages in multilateral and bilateral discussions to further international computer security awareness and policy development, as well as incident response team information-sharing and capacity-building objectives. DHS engages in bilateral discussions on cyber security issues with various international partners, such as India, Italy, Japan, and Norway. DHS also works with international partners in multilateral and regional forums to address cyber security and critical information infrastructure protection. For example, the Asia-Pacific Economic Cooperation Telecommunications Working Group recently engaged in a capacity-building program to help member countries develop computer emergency response teams. The OAS has approved a framework proposal by its Cyber Security Working Group to create an OAS regional computer incident response contact network for information sharing and capacity building. Multilateral collaboration to build a global culture of security includes participation in the OECD, G8, and the United Nations. Many of these countries and organizations have developed mechanisms for engaging the private sector in dialogue and program efforts.
- **Collaboration on Cyber Crime:** The U.S. outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe Convention on Cyber Crime, as well as: (1) G8 High-Tech Crime Working Group's principles for fighting cyber crime and protecting critical information infrastructure, (2) OECD guidelines on information and network security, and (3) United Nations General Assembly resolutions based on the G8 and OECD efforts. The goal of this outreach strategy is to encourage foreign governments and regional organizations to join the United States in efforts to protect internationally interconnected systems.
- **Collaborative Efforts for Cyber Watch Warning and Incident Response:** The United States works with key allies on cyber security policy and operational cooperation. Leveraging pre-existing relationships among Computer Security Incident Response Teams (CSIRTs), DHS has established a preliminary framework for cooperation on cyber security policy, watch and warning, and incident response with Australia, Canada, New Zealand, and the United Kingdom. The framework also incorporates efforts on strategic issues as agreed upon by these allies. DHS is also participating in the establishment of an International Watch and Warning Network (IWWN) among cyber security policy, computer emergency response, and law enforcement participants from 15 countries. The IWWN will provide a mechanism for the participating countries to share information to build global cyber situational awareness and coordinate incident response.
- **Partnerships to Address Cyber Aspects of** CI/KR **Protection:** The Federal Government leverages existing agreements such as the SPP and the JCG with the United Kingdom to address the Information Technology sector and cross-cutting cyber security as part of CI/KR protection. The trilateral SPP builds on existing bilateral agreements between the United States and Canada and the United States and Mexico by providing a forum to address issues on a dual bi-national basis. In the context of the JCG, DHS established an action plan to address cyber security, watch, warning, and incident response, and other strategic initiatives.

4.1.4.4 Foreign Investment in CI/KR

CI/KR protection may be affected by foreign investment and ownership of sector assets. This issue is monitored at the Federal level by the CFIUS. The committee provides a forum for assessing the impacts of proposed foreign investments on CI/KR protection, government monitoring activities aimed at ensuring compliance with agreements that result from CFIUS rulings, and supporting executive branch reviews of telecommunications applications to the FCC from foreign entities to assess if they pose any national security threat to CI/KR (see appendix 1B.4.4).

4.2 Information Sharing: A Network Approach

The effective implementation of the NIPP is predicated on active participation by government and private sector security partners in robust multi-directional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to CI/KR and participate in ongoing multi-directional information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced. Similarly, when the government is equipped with an understanding of private sector information needs, it can

adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

The NIPP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decisionmaking and actions. The objectives of the network approach are to:

- Enable secure multi-directional information sharing between and across government and industry that focuses, streamlines, and reduces redundant reporting to the greatest extent possible;
- Implement a common set of communications, coordination, and information-sharing capabilities for all security partners;
- Provide security partners with a robust communications framework tailored to their specific information-sharing requirements, risk landscape, and protective architecture;
- Provide security partners with a comprehensive common operating picture that includes timely and accurate information about natural hazards, general and specific terrorist threats, incidents and events, impact assessments, and best practices;
- Provide security partners with timely incident reporting and verification of related facts that CI/KR owners and operators can use with confidence when considering how evolving incidents might affect their security posture;
- Provide a means for State, local, tribal, and private sector security partners to be integrated, as appropriate, into the intelligence cycle, to include providing inputs to the intelligence requirements development process;
- Enable the flow of information required for security partners to assess risks, conduct risk management activities, invest in security measures, and allocate resources; and
- Protect the integrity and confidentiality of sensitive information.

The information-sharing process is designed to communicate both actionable information on threats and incidents and information pertaining to overall CI/KR status (e.g., plausible threats, vulnerabilities, potential consequences, incident situation, and recovery progress) so that owners and operators, States, localities, tribal governments, and other security partners can assess risks, make appropriate security investments, and take effective and efficient protective actions.

4.2.1 Information Sharing Between NIPP Security Partners

The primary objective of the NIPP network approach to information sharing is to enhance situational awareness and maximize the ability of government and private sector security partners at all levels to assess risks and execute risk-mitigation programs and activities. Implementation of the Nation's CI/KR protection mission depends on the ability of the government to receive and provide timely, actionable information on emerging threats to CI/KR owners and operators and security professionals so that they can take the necessary steps to mitigate risk.

Ongoing and future initiatives generally fall within one of three overarching categories:

- **Planning:** All security partners have a stake in setting the individual information requirements that best suit the needs of each CI/KR sector. DHS, in conjunction with SSAs and other State, local, tribal, and private sector security partners, will collaboratively develop and disseminate an Annual CI/KR Protection Information Requirements Report that summarizes the sectors' input and makes recommendations for collecting information requirements. The Information Requirements Report will be disseminated to the sectors through the SCCs. In addition to this process, DHS will coordinate with the Intelligence Community to support information collection that reflects the emerging requirements provided by SSAs and State, local, tribal, and private sector partners.
- **Information Collection:** Private sector participation in information collection is voluntary and includes providing subject matter expertise and operational, vulnerability, and consequence data. Private sector partners also report suspicious activity that could signal pre-operational terrorist activity to the DHS National Operations Center (NOC) through the National Infrastructure Coordinating Center (NICC). Information shared by the private sector, including that which is protected by PCII or other approaches, is integrated with government-collected information to produce comprehensive threat assessments and threat warning products. DHS assessments, excluding PCII information, are shared across the sectors through electronic dissemination, posting to Homeland Security Information Network (HSIN) portals, and direct outreach by DHS/OIP sector specialists and DHS/HITRAC analysts. These efforts provide the private sector with timely, actionable information to enhance situational awareness and enable security planning activities.

- **Analysis and Decisionmaking:** DHS/HITRAC is responsible for integrating CI/KR specific vulnerability and consequence data with threat information to produce actionable risk assessments used to inform CI/KR risk-mitigation activities at all levels. DHS/HITRAC analysts work closely with CI/KR sector subject matter experts to ensure that these products address the individual requirements of each sector and help actuate corresponding security activities.

4.2.2 Information-Sharing Life Cycle

Planning, information collection, analyses, and decisionmaking are key elements of the CI/KR information life cycle. Protection of sensitive information and dissemination of actionable information are central tenets that are maintained throughout each stage of the life cycle.

4.2.2.1 Information Requirement

The information-sharing process begins with defining the information collection requirements to be adopted by field entities, analytic entities, and all other security partners that collect and disseminate intelligence and other security-related information.

4.2.2.2 Balancing the Sharing and Protection of Information

Effective information sharing relies on the balance between making information available, and the ability to protect information that may be sensitive, proprietary, or that the disclosure of which might compromise ongoing law enforcement, intelligence, or military operations or methods.

Distribution of information is based on using appropriate protocols for information protection. Whether the sharing is top-down (by partners working with national-level information such as system-wide aggregate data or the results of emergent threat analysis from the Intelligence Community) or bottom-up (by field officers or facility operators sharing detailed and location-specific information), the network approach places shared responsibility on all security partners to maintain appropriate and protected information-sharing practices.

4.2.2.3 Top-Down and Bottom-Up Sharing

During incident situations, DHS monitors risk management activities and CI/KR status at the functional/operations level, the local law enforcement level, and at the cross-sector level. Information sharing may also incorporate information that comes from pre- and post-event natural disaster warnings and reports.

Top-Down Sharing: Under this approach, information regarding a potential terrorist threat originates at the national level through domestic and/or overseas collection and fused analysis, and subsequently is routed to State and local governments, CI/KR owners and operators, and other Federal agencies for immediate attention and/or action. This type of information is generally assessed against DHS analysis reports and integrated with CI/KR-related information and data from a variety of government and private sector sources. The result of this integration is the development of timely information products, often produced within hours, that are available for appropriate dissemination to security partners, based on previously specified reporting processes and data formats.

Bottom-Up Sharing: State, local, tribal, private sector, and nongovernmental organizations report a variety of security- and incident-related information from the field using established communications and reporting channels. This bottom-up information is assessed by DHS and its partners in the intelligence and law enforcement communities in the context of threat, vulnerability, consequence, and other information to illustrate a comprehensive risk landscape.

Threat information that is received from local law enforcement or private sector suspicious activity reporting is routed to DHS through the NICC and the NOC. The information is then routed to intelligence and operations personnel, as appropriate, to support further analysis or action as required. In the context of evolving threat or incident situations, further national-level analyses may result in the development and dissemination of a variety of HITRAC products as discussed in chapter 3. Further information-sharing and incident management activities are based on the specific analysis and needs of these operations personnel.

DHS also monitors operational information such as changes in local risk management measures, pre- and post-incident disaster or emergency response information, and local law enforcement activities. Monitoring local incidents contributes to a comprehensive picture that supports incident-related damage assessment, restoration prioritization, and other national- or regional-level planning or resource allocation efforts. Written products and reports that result from the ongoing monitoring are shared with relevant security partners according to appropriate information protection protocols.

4.2.2.4 Decisions and Actions

Information sharing, whether top-down or bottom-up, is a means to an end. The objective of the information-sharing life cycle is to provide timely and relevant information that

Figure 4-2: NIPP Networked Information-Sharing Approach

security partners can use to make decisions and take necessary actions to manage CI/KR risk.

4.2.3 The Information-Sharing Approach

Figure 4.2 illustrates the broad concept of the NIPP multi-directional networked information-sharing approach. This information-sharing network consists of components that are connected by a national Web-based communications platform, known as the HSIN, so that security partners can obtain, analyze, and share information. The diagram illustrates how the HSIN is used for two-way and multi-directional information sharing between DHS; the Federal Intelligence Community; Federal departments and agencies; State, local, and tribal jurisdictions; and the private sector. The connectivity of the network also allows these partners to share information and coordinate among themselves (e.g., State-to-State coordination). Security partners are grouped into nodes in the information-sharing network approach.

4.2.3.1 Information Sharing With HSIN

When fully deployed, the HSIN will constitute a robust and significant information-sharing system that supports NIPP-related steady-state CI/KR protection and NRP-related incident management activities, as well as serving the information-sharing processes that form the bridge between these two homeland security missions. The linkage between the nodes results in a dynamic view of the strategic risk and evolving incident landscape. HSIN functions as one of a number of mechanisms that enable DHS, SSAs, and other security partners to share information. Other supporting technologies and more traditional methods of communications will continue to support CI/KR protection, as appropriate, and will be fully integrated into the network approach.

DHS and the SSAs work with other security partners to measure the efficacy of the network and to identify areas in which new mechanisms or supporting technologies are required. The HSIN and the key nodes of the NIPP information-sharing approach are detailed in the subsequent sections. By offering a user-friendly, efficient conduit for information sharing, HSIN enhances the combined effectiveness of all security partners in an all-hazards environment. HSIN network architecture design is informed by experience gained by DOD and other Federal agencies in developing networks to support similar missions. It supports a secure common operating picture for all security partner command or watch centers, including those of supporting emergency management and public health activities.

As specified in the Intelligence Reform and Terrorism Prevention Act of 2004, the Federal Government is working with State and local partners and the private sector to create the information-sharing environment (ISE) for terrorism information, in which access to such information is matched to the roles, responsibilities, and missions of all organizations engaged in countering terrorism and is timely and relevant to their needs. HSIN will be one part of the ISE, and when fully developed, users of HSIN will be able to access ISE terrorism information based on their roles, responsibilities, and missions.

The HSIN is composed of multiple, non-hierarchal communities of interest (COIs) that offer security partners the means to share information based on secure access. COIs provide virtual areas where groups of participants with common concerns, such as law enforcement, counterterrorism, critical infrastructure, emergency management, intelligence, international, and other topics, can share information. This structure allows government and industry partners to engage in collaborative exchanges, based on specific information requirements, mission emphasis, or interest level. Within the Homeland Security Information Network for Critical Sectors (HSIN-CS) COI, each sector establishes rules for participation, including vetting and verification processes that are appropriate for the sector CI/KR landscape and requirements for information protection. For example, in some sectors, applicants are vetted through the SCC or ISAC; others may require participants to be documented members of a specific profession, such as law enforcement.

4.2.4 The Federal Intelligence Node

The Federal Intelligence Node, comprised of national Intelligence Community agencies, SSA intelligence offices, and the DHS Office of Intelligence and Analysis (DHS/OI&A), identifies and establishes the credibility of general and specific threats. This node also includes national, regional, and field-level information-sharing and intelligence fusion center entities that contribute to information sharing in the context of the CI/KR protection mission.

At the national level, these centers include, but are not limited to, the DHS/HITRAC, the FBI-led National Joint Terrorism Task Force (NJTTF), the National Counterterrorism Center (NCTC), and the National Maritime Intelligence Center.

- **DHS/HITRAC** analyzes and integrates threat information and works closely with components of the Federal Infrastructure Node to generate and disseminate threat warning products to security partners, both internal and external to the network, as appropriate.
- The **NJTTF** mission is to enhance communications, coordination, and cooperation among Federal, State, local, and tribal agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, and homeland security communities by providing a point of fusion for terrorism intelligence and by supporting Joint Terrorism Task Forces (JTTFs) throughout the United States.

Project Seahawk is a task force comprised of 40 Federal, State, and local law enforcement agencies that enhances intermodal transportation and port security by sharing jurisdictional responsibility for the Port of Charleston and its metropolitan area. Other examples of information-sharing and intelligence fusion center entities include:

- DHS/USCG operates a Maritime Intelligence Fusion Center (MIFC)—Pacific (Alameda, CA) and an MIFC—Atlantic (Dam Neck, VA). These centers serve as resources for intelligence support for the DHS/USCG, as well as for local and international maritime, intelligence, and law enforcement partners;
- DHS/Immigration and Customs Enforcement operates the Human Smuggling and Trafficking Center, an interagency joint intelligence fusion center focused specifically on human smuggling and human trafficking. Other DHS entities, the Department of State, DOJ, and other members of the Intelligence Community participate in the Center; and
- The Defense Intelligence Agency operates intelligence analytic fusion centers in the various overseas areas of operation (i.e., EUCOM, PACOM, CENTCOM, SOUTHCOM, NORTHCOM). These fusion cells support production coordination and targeting/operational activities, as well as ongoing area operations or special programs.

- The **NCTC** serves as the primary Federal organization for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to terrorism and counterterrorism, except purely domestic counterterrorism information. The NCTC may, consistent with applicable law, receive, retain, and disseminate information from any Federal, State, or local government or other source necessary to fulfill its responsibilities.
- The **National Maritime Intelligence Center** serves as the central point of connectivity to fuse, analyze, and disseminate information and intelligence for shared situational awareness across classification boundaries.

At the regional and field levels, Federal information-sharing and intelligence fusion centers include entities such as the local JTTFs, the DHS/DOJ-sponsored Project Seahawk, and FBI Field Intelligence Groups that provide the centralized intelligence/information-sharing component in every FBI field office.

4.2.5 The Federal Infrastructure Node

The Federal Infrastructure Node, comprised of DHS, SSAs, and other Federal departments and agencies, gathers and receives threat, incident, and other operational information from a variety of sources (including a wide range of watch/operations centers). This information enables assessment of the status of CI/KR and facilitates the development and dissemination of appropriate real-time threat and warning products and corresponding protective measures recommendations to security partners (see chapter 3). Participants in the Federal node collaborate with CI/KR owners and operators to gain input during the development of threat and warning products and corresponding protective measures recommendations.

4.2.6 State, Local, Tribal, and Regional Node

This node provides links between DHS, the SSAs, and security partners at the State, local, regional, and tribal levels. Several established communications channels provide protocols for passing information from the local to the State to the Federal level and disseminating information from the Federal Government to other security partners. The NIPP network approach augments these established communications channels by facilitating two-way and multi-directional information sharing between various security partners. Members of this node provide incident response, first-responder information, and reports of suspicious activity to the FBI and DHS for purposes of awareness and analysis. Homeland security advisors receive and further disseminate coordinated DHS/FBI threat and warning products, as appropriate.

Numerous States and urban area jurisdictions also have established fusion centers or terrorism early warning centers to facilitate a collaborative process between law enforcement, public safety, other first-responders, and private entities to collect, integrate, evaluate, analyze, and disseminate criminal intelligence and other information that relates to CI/KR protection.

Additionally, DHS protective security advisors (PSAs) serve as liaisons to CI/KR owners and operators, as well as State, local, and tribal officials. PSAs assist efforts to identify, assess, monitor, and minimize risk to CI/KR at the regional, State, or local level. PSAs facilitate, coordinate, and/or perform vulnerability assessments in support of local CI/KR owners and operators, and assist with security efforts coordinated through State homeland security advisors, as requested by State, local, or tribal authorities.

4.2.7 Private Sector Node

The Private Sector Node includes CI/KR owners and operators, SCCs, ISACs, and trade associations that provide incident information, as well as reports of suspicious activity that may indicate actual or potential criminal intent or terrorist activity. DHS, in return, provides all-hazards warning products, recommended protective measures, and alert notification to a variety of industry coordination and information-sharing mechanisms, as well as directly to affected CI/KR owners and operators.

The NIPP network approach connects and augments existing information-sharing mechanisms, where appropriate, to reach the widest possible population of CI/KR owners and operators and other security partners. Owners and operators need accurate and timely incident and threat-related information in order to effectively manage risk; enable post-event restoration and recovery; and make decisions regarding protective strategies, partnerships, mitigation plans, security measures, and investments for addressing risk.

ISACs provide an example of an effective private sector information-sharing and analysis mechanism. Originally recommended by Presidential Decision Directive 63 (PDD-63) in 1998, ISACs are sector-specific entities that advance physical and cyber CI/KR protection efforts by establishing and maintaining frameworks for operational interaction between and among members and external security partners. ISACs typically serve as the tactical and operational arms for sector information-sharing efforts.

ISAC functions include, but are not limited to, supporting sector-specific information/intelligence requirements for incidents, threats, and vulnerabilities; providing secure capability for members to exchange and share information on cyber, physical, or other threats; establishing and maintaining operational-level dialogue with appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness.

The sector partnership model recognizes that not all CI/KR sectors have established ISACs. Each sector has the ability to implement a tailored information-sharing solution that may include ISACs; voluntary standards development organizations; or other mechanisms, such as trade associations, security organizations, and industry-wide or corporate operations centers, working in concert to expand the flow of knowledge exchange to all infrastructure owners and operators. Most ISACs are members of the ISAC Council, which provides the mechanism for the inter-sector sharing of operational information. Sectors that do not have ISACs per se use other mechanisms that participate in the HSIN and other CI/KR protection information-sharing arrangements. For the purposes of the NIPP, these operationally oriented groups are also referred to collectively as ISACs.

ISACs vary greatly in composition (i.e., membership), scope (e.g., focus and coverage within a sector), and capabilities (e.g., 24/7 staffing and analytical capacity), as do the sectors they serve. As the sectors define and implement their unique information-sharing mechanisms for CI/KR protection, the ISACs will remain an important information-sharing mechanism for many sectors under the NIPP partnership model.

4.2.8 DHS Operations Node

The DHS Operations Node maintains close working relationships with other government and private sector security partners to enable and coordinate an integrated operational picture, provide operational and situational awareness, and facilitate CI/KR information sharing within and across sectors. DHS and other Federal watch/operations centers provide the 24/7 capability required to enable the real-time alerts and warnings, incident reporting, situational awareness, and assessments needed to support CI/KR protection.

The principal purpose of a watch/operations center is to collect and share information. Therefore, the value and effectiveness of such centers is largely dependent upon a timely, accurate, and extensive population of information sources. The NIPP information-sharing network approach virtually integrates numerous primary watch/operations centers at various levels to enhance information exchange with security partners, providing a far-reaching network of awareness and coordination.

4.2.8.1 National Operations Center[21]

The NOC, formerly known as the Homeland Security Operations Center, serves as the Nation's hub for domestic incident management operational coordination and situational awareness. The NOC is a standing 24/7 interagency organization fusing law enforcement, national intelligence, emergency response, and private sector reporting. The NOC facilitates homeland security information-sharing and operational coordination among Federal, State, local, tribal, and private sector partners, as well as select members of the international community. As such, it is at the center of the NIPP information-sharing network.

The NOC information-sharing and coordination functions include:

- **Information Collection and Analysis:** The NOC maintains national-level situational awareness and provides a centralized, real-time flow of information among security partners. An NOC common operating picture is generated using data collected from across the country to provide a broad view of the Nation's current overall risk and preparedness status. Using the common operating picture, NOC personnel, in coordination with the FBI and other agencies, as appropriate, perform initial assessments to gauge the terrorism nexus and track actions taking place across the country in response to a threat, natural disaster, or accident. The information compiled by the NOC is distributed to partners, as appropriate, and is accessible to affected security partners through the HSIN.
- **Situational Awareness and Incident Response Coordination:** The NOC provides the all-hazards information needed to help make decisions and define courses of action.
- **Threat Warning Products:** DHS jointly reviews threat information with partners in the FBI, Intelligence Community, and other Federal departments and agencies on a continuous basis. When a threat is determined to be credible and actionable, DHS is responsible for coordinating with these Federal partners in the development and dissemination of threat warning products. This coordination ensures, to the greatest extent possible, the accuracy and timeliness of the information, as well as concurrence by Federal partners.

[21] *The Federal Response to Hurricane Katrina: Lessons Learned*, issued by the Homeland Security Council, February 2006, recommended the establishment of the NOC as a single entity to unify situational awareness and response, recovery, and mitigation functions. The NOC replaces the DHS Homeland Security Operations Center.

DHS disseminates threat warning products to Federal, State, local, and tribal governments, as well as to private sector organizations and international partners as COI members through the HSIN, established e-mail distribution lists, and other methods, as required:

- **Threat Advisories:** Contain actionable threat information and provide recommended protective actions based on the nature of the threat. They also may communicate a national, regional, or sector-specific change in the level of the HSAS.
- **Homeland Security Assessments:** Communicate threat information that does not meet the timeliness, specificity, or criticality criteria of an advisory, but is pertinent to the security of U.S. CI/KR.

The NOC is comprised of four sub-elements: the NOC Headquarters Element (NOC-HQE), the National Response Coordination Center (NRCC), the intelligence and analysis element, and the NICC.

- **NOC Headquarters Element:** The NOC-HQE is a multi-agency center that provides overall Federal prevention, protection, and preparedness coordination. The NOC-HQE integrates representatives from DHS and other Federal departments and agencies to support steady-state threat-monitoring requirements and situational awareness, as well as operational incident management planning and coordination. The organizational structure of the NOC-HQE is designed to integrate a full spectrum of interagency subject matter expertise, operational planning capability, and reach-back capability to meet the demands of a wide range of potential incident scenarios.
- **National Response Coordination Center:** The NRCC is a multi-agency center that provides overall coordination of Federal response, recovery, and mitigation activities, and emergency management program implementation.
- **Intelligence and Analysis Element:** The intelligence and analysis element is responsible for interagency intelligence collection requirements, analysis, production, and product dissemination for DHS, to include homeland security threat warnings, advisory bulletins, and other information pertinent to national incident management (see section 4.2.4).
- **National Infrastructure Coordinating Center:** The NICC is a 24/7 watch/operations center that maintains ongoing operational and situational awareness of the Nation's CI/KR sectors. As a CI/KR-focused element of the NOC, the NICC provides a centralized mechanism and process for information sharing and coordination between the government, SCCs, GCCs, and other industry partners. The NICC receives situational, operational, and incident information from the CI/KR sectors, in accordance with information-sharing protocols established in the NRP. The NICC also disseminates products originated by HITRAC that contain all-hazards warning, threat, and CI/KR protection information:
  - **Alerts and Warnings:** The NICC disseminates threat-related and other all-hazards information products to an extensive customer base of private sector partners.
  - **Suspicious Activity and Potential Threat Reporting:** The NICC receives and processes reports from the private sector on suspicious activities or potential threats to the Nation's CI/KR. The NICC documents the information provided, compiles additional details surrounding the suspicious activity or potential threat, and forwards the report to DHS sector specialists, the NOC, HITRAC, and the FBI.
  - **Incidents and Events:** When an incident or event occurs, the NICC coordinates with DHS sector specialists, industry partners, and other established information-sharing mechanisms to communicate pertinent information. As needed, the NICC generates reports detailing the incident, as well as the sector impacts (or potential impacts), and disseminates them to the NOC.
  - **National Response Planning and Execution:** The NICC supports the NRP by facilitating information sharing among SCCs, GCCs, ISACs, and other security partners during CI/KR mitigation, response, and recovery activities.

4.2.8.2 National Coordinating Center for Telecommunications

Pursuant to Executive Order 12472, the National Communications System (NCS) assists the President, National Security Council, Homeland Security Council, Office of Science and Technology Policy (OSTP) and OMB in the coordination and provision of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. As called for in the Executive order, the NCS has established the NCC, which is a joint industry-government entity. Under the Executive order, the NCC assists the NCS in the initiation, coordination, restoration, and reconstitution of national security or emergency preparedness communications services or facilities under all conditions of crisis or emergency. The NCC regularly monitors the status of communications systems. It collects situational

and operational information on a regular basis, as well as during a crisis, and provides information to the NCS. The NCS, in turn, shares information with the White House and other DHS components.

4.2.8.3 United States Computer Emergency Readiness Team

The United States Computer Emergency Readiness Team (US-CERT) is a 24/7 single point of contact for cyberspace analysis, warning, information sharing, and incident response and recovery for security partners. It is a partnership between DHS and the public and private sectors designed to enable protection of cyber infrastructure and to coordinate the prevention of and response to cyber attacks across the Nation.

US-CERT coordinates with security partners to disseminate reasoned and actionable cyber security information through a Web site, accessible via the HSIN, and through mailing lists. Among the products it provides are:

- **Cyber Security Bulletins:** Weekly bulletins written for systems administrators and other technical users that summarize published information concerning new security issues and vulnerabilities.
- **Technical Cyber Security Alerts:** Written for system administrators and experienced users, technical alerts provide timely information on current security issues, vulnerabilities, and exploits.
- **Cyber Security Alerts:** Written in a language for home, corporate, and new users, these alerts are published in conjunction with technical alerts when there are security issues that affect the general public.
- **Cyber Security Tips:** Tips provide information and advice on a variety of common security topics. They are published biweekly and are primarily intended for home, corporate, and new users.
- **National Web Cast Initiative:** DHS, through US-CERT and the Multi-State Information Sharing and Analysis Center (MS-ISAC), has initiated a joint partnership to develop a series of national Web casts that will examine critical and timely cyber security issues. The purpose of the initiative is to strengthen the Nation's cyber readiness and resilience.

US-CERT also provides a method for citizens, businesses, and other important institutions to communicate and coordinate directly with the Federal Government on matters of cyber security. The private sector can use the protections afforded by the Critical Infrastructure Information Act to electronically submit proprietary data to US-CERT.

4.2.9 Other Information-Sharing Nodes

DHS, other Federal agencies, and the law enforcement community provide additional services and programs that share information supporting CI/KR protection with a broad range of security partners. These include, but are not limited to, the following:

- **Sharing National Security Information:** DHS sponsors security clearances for designated private sector owners and operators to promote the sharing of classified information using currently available methods and systems.
- **FBI Law Enforcement Online (LEO):** LEO can be accessed by any approved employee of a Federal, State, or local law enforcement agency, or approved member of an authorized law enforcement special interest group. LEO provides a communications mechanism to link all levels of law enforcement throughout the United States.
- **RISSNET™** is a secure nationwide law enforcement and information-sharing network that operates as part of the Regional Information Sharing Systems (RISS) Program. RISS is composed of six regional centers that share intelligence and coordinate efforts targeted against criminal networks, terrorism, cyber crime, and other unlawful activities that cross jurisdictional lines. RISSNET features include online access to a RISS electronic bulletin board, databases, RISS center Web pages, secure e-mail, a RISS search engine, and other center resources. The RISS program is federally funded and administered by the DOJ/Bureau of Justice Assistance.
- **FBI InfraGard:** InfraGard is a partnership between the FBI, other government entities, and the private sector. The InfraGard National Membership Alliance is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants that enables the sharing of knowledge, expertise, information, and intelligence related to the protection of U.S. CI/KR from physical and cyber threats.
- **Interagency Cyber Security Efforts:** The intelligence and law enforcement communities have various information-sharing mechanisms in place. Examples include:
  - **U.S. Secret Service's Electronic Crimes Task Forces:** U.S. Secret Service's Electronic Crimes Task Forces (ECTFs) prevent, detect, and investigate electronic crimes, cyber-based attacks, and intrusions against CI/KR and electronic payment systems, and provide interagency information sharing on related issues.

– **Cybercop Portal:** The DHS-sponsored Cybercop portal is a secure Internet-based information-sharing mechanism that connects more than 5,300 members of the law enforcement community, bank investigators, and the network security specialists involved in electronic crimes investigations.

- **CEO COM LINK℠:** The Critical Emergency Operations Communications Link (CEO COM LINK) is a telephone communications system that will enable the Nation's top chief executive officers (CEOs) to enhance the protection of employees, communities, and the Nation's CI/KR by communicating with government officials and each other about specific threats or during national crises. The calls, which are restricted to authorized participants, allow top government officials to brief CEOs on developments and threats, and allow CEOs to ask questions or share information with government leaders and with each other.

4.3 Protection of Sensitive CI/KR Information

NIPP implementation will rely greatly on critical infrastructure information provided by the private sector. Much of this is sensitive business or security information that could cause serious damage to companies, the economy, and public safety or security through unauthorized disclosure or access to this information.

The Federal Government has a statutory responsibility to safeguard information collected from or about CI/KR activities. Section 201(d)(12)(a) of the Homeland Security Act requires DHS to "ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties." DHS and other Federal agencies use a number of programs and procedures, such as the PCII Program, to ensure that CI/KR information is properly safeguarded. In addition to PCII, other programs and procedures used to protect sensitive information include Sensitive Security Information for transportation activities, Unclassified Controlled Nuclear Information (UCNI), contractual provisions, classified national provisions, Classified National Security Information, Law Enforcement Sensitive Information, Federal Security Information Guidelines, Federal Security Classification Guidelines, and other requirements established by law.

4.3.1 Protected Critical Infrastructure Information Program

The PCII Program was established pursuant to the Critical Infrastructure Information Act of 2002. The program provides a means for sharing private sector information with the government while providing assurances that the information will be exempt from public disclosure and will be properly safeguarded. This enables members of the private sector to voluntarily submit sensitive information regarding CI/KR to DHS with the assurance that the information will be protected.

The PCII Program, which operates under the authority of the Critical Infrastructure Information (CII) Act and interim implementing regulations (6 Code of Federal Regulations (CFR) Part 29 (the Interim Rule)), defines the requirements for submitting CII and the requirements that government entities must meet for accessing and safeguarding PCII. DHS remains committed to making PCII an effective tool for robust information sharing between critical infrastructure owners and operators and the government, and is presently working on rulemaking that will replace the interim regulations and make the program even stronger. For more information, contact the PCII Program Office at pcii-info@dhs.gov. Additional PCII Program information may also be found at www.dhs.gov/pcii.

4.3.1.1 PCII Program Office

The PCII Program Office is responsible for managing PCII program requirements, developing protocols for handling PCII, raising awareness of the need for protected information sharing between government and the private sector, and assuring that programs receiving voluntary submissions of PCII use proper procedures to continuously safeguard that information. The Program Office works with government organizations and the private sector to develop information-sharing partnerships that promote greater homeland security through validated protection programs and procedures.

4.3.1.2 Critical Infrastructure Information Protection

The following process and procedures apply to all CII submissions:

- Individuals or collaborative groups may submit information for protection;
- The PCII Program Office validates that the information qualifies for protection under the act;

- All validated PCII is stored in a secure data management system and security partners follow DHS sharing guidelines for unclassified but sensitive information;
- Secure methods are used for disseminating PCII;
- Authorized users must comply with safeguarding requirements defined by the PCII Program Office; and
- Any suspected disclosure of PCII will be promptly investigated.

4.3.1.3 Uses of PCII

PCII may be shared with authorized government entities, including Federal, State, or local government employees or contractors supporting Federal agencies, only for the purposes of securing CI/KR and protected systems. PCII will be used for analysis, prevention, response, recovery, or reconstitution of CI/KR threatened by terrorism or other hazards.

Authorized government entities may generate advisories, alerts, and warnings relevant to the private sector based on the information provided; however, communications made available to the public will not contain any sensitive information provided by the submitter. PCII can be combined with other information, including classified information, in support of CI/KR protection activities; in such cases, PCII used in such products must be marked accordingly.

The CII Act specifically authorizes disclosure of PCII without the permission of the submitter:

- In furtherance of an investigation or the prosecution of a criminal act;
- To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee, or any such joint committee; or
- To the Comptroller General or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

4.3.1.4 PCII Protections and Authorized Users

The PCII Program has established procedures to ensure that PCII is properly accessed, used, and safeguarded throughout its life cycle. These safeguards ensure that submitted information is:

- Used appropriately for homeland security purposes;
- Accessed only by authorized and properly trained staff who have a need to know;
- Protected from disclosure under the Freedom of Information Act (FOIA) and similar State and local disclosure laws, and from use in civil litigation and regulatory actions; and
- Safeguarded and handled in a secure manner.

The law and rule prescribe criminal penalties for intentional unauthorized access, distribution, and misuse of PCII including the following provisions:

- Federal employees may be subject to disciplinary action, including criminal and civil penalties and loss of employment;
- Contract employees may face termination and the contractor may have its contract terminated; and
- The sanctions provided for under the CII Act for unauthorized disclosure of PCII apply only to Federal personnel. State and local participating entities may have their own penalties for improperly handling sensitive information and these entities may lose future access to PCII.

4.3.2 Other Information Protection Protocols

Information protection protocols may impose requirements for access or other standard processes for safeguarding information. Information need not be designated as CII to receive security protection and disclosure restrictions. Several categories of information related to CI/KR are considered to be sensitive but unclassified and require protection. Examples include sector-specific information, such as sensitive transportation or nuclear information, or information determined to be classified information based on the analysis of unclassified information. The major categories that apply to CI/KR are discussed below.

4.3.2.1 Sensitive Security Information

The Maritime Transportation Security Act, the Aviation Transportation Security Act, and the Homeland Security Act establish protection for Sensitive Security Information (SSI). TSA and the USCG may designate information as SSI when disclosure would:

- Be detrimental to security;
- Reveal trade secrets or privileged or confidential information; or
- Constitute an unwarranted invasion of privacy.

Parties accessing SSI must demonstrate a need to know. Holders of SSI must protect such information from unauthorized disclosure and must destroy the information when it is no longer needed. SSI protection pertains to government officials as well as to transportation sector owners and operators.

4.3.2.2 Unclassified Controlled Nuclear Information

DOD and DOE may designate certain information as UCNI. Such information relates to the production, processing, or use of nuclear material; nuclear facility design information; and security plans and measures for the physical protection of nuclear materials. This designation is used when disclosure could affect public health and safety or national security by enabling illegal production or diversion of nuclear materials or weapons. Access to UCNI is restricted to those who have a need to know. Procedures are specified for marking and safeguarding UCNI.

4.3.2.3 Freedom of Information Act Exemptions and Exclusions

FOIA was enacted in 1966 and amended and modified by Congress in legislation, including the Electronic Freedom of Information Act of 1996 and the Privacy Act of 1974. The act established a statutory right of public access to executive branch information in the Federal Government and generally provides that any person has a right, enforceable in court, to obtain access to Federal agency records. Certain records may be protected from public disclosure under the act if they fall into one of three special law enforcement exclusions that protect information such as the name of informants. They may also be protected from public disclosure under the act if they are in one of nine exemption categories that protect such information as classified national security data, trade secrets, or financial information obtained by the government from individuals, personnel and medical files, and CI/KR information.

4.3.2.4 Classified Information

Under Executive Order 12958, as amended, and Executive Order 12829, as amended, the Information Security Oversight Office of the National Archives is responsible to the President for overseeing the security classification programs in both government and industry that safeguard National Security Information (NSI), including information related to defense against transnational terrorism.

Classified information is a special category of sensitive information that is accorded special protections and access controls. It has certain characteristics that distinguish it from other sensitive information. These include:

- The information can only be designated as classified by a duly empowered authority;
- The information must be owned by, produced by or for, or under the control of the Federal Government;
- The unauthorized disclosure of the information reasonably could be expected to result in identifiable damage to U.S. national security; and
- Only information related to the following may be classified:
  - Military plans, weapons systems, or operations;
  - Foreign government information;
  - Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
  - Foreign relations or foreign activities of the United States, including confidential sources;
  - Scientific, technological, or economic matters related to national security, which includes defense against transnational terrorism;
  - Federal Government programs for safeguarding nuclear materials or facilities;
  - Vulnerabilities or capabilities of systems, installations, infrastructure, projects, plans, or protection services related to national security, which includes defense against transnational terrorism; or
  - Weapons of mass destruction.

Many forms of information related to CI/KR protection have these characteristics. This information may be determined to be classified information and protected accordingly.

4.3.2.5 Physical and Cyber Security Measures

DHS uses strict information security protocols for the access, use, and storage of sensitive information, including that related to CI/KR. These protocols include both physical security measures and cyber security measures. Physical security protocols for DHS facilities require access control and risk-mitigation measures. Information security protocols include access controls, login restrictions, session tracking, and data labeling. Appendix 3C provides a discussion of these protections as applied to the NADB.

4.4 Privacy and Constitutional Freedoms

Mechanisms detailed in the NIPP are designed to provide a balance between achieving a high level of security and protecting the civil rights and liberties that form an integral part of America's national character. Achieving this balance requires acceptance of some level of risk. In providing for effective protective programs, the processes outlined in the NIPP respect privacy, freedom of expression, freedom of movement, freedom from unlawful discrimination, and other liberties that define the American way of life.

Compliance with the Privacy Act and governmental privacy regulations and procedures is a key factor that is considered when collecting, maintaining, using, and disseminating personal information. The following DHS offices support the NIPP processes:

- **DHS Privacy Office:** Pursuant to the Homeland Security Act, DHS has designated a privacy officer to ensure that it appropriately balances the mission with civil liberty and privacy concerns. The officer consults regularly with privacy advocates, industry experts, and the public at large to ensure broad input and consideration of privacy issues so that DHS achieves solutions that protect privacy while enhancing security.
- **DHS Office for Civil Rights and Civil Liberties:** Pursuant to the Homeland Security Act, DHS has established an Office for Civil Rights and Civil Liberties to review and assess allegations of abuse of civil rights or civil liberties, racial or ethnic profiling, and to provide advice to DHS components.

5. Integrating CI/KR Protection as Part of the Homeland Security Mission

This chapter describes the linkages between the NIPP, the SSPs, and other CI/KR protection strategies, plans, and initiatives that are most relevant to the overarching national homeland security and CI/KR protection missions. It also describes how the unified national CI/KR protection effort integrates with the prevention, protection, response, and recovery elements of the homeland security mission. Sector-specific linkages to these other national frameworks are more appropriately addressed in the SSPs.

5.1 A Coordinated National Approach to the Homeland Security Mission

The NIPP provides the structure needed to coordinate, integrate, and synchronize activities derived from various relevant statutes, national strategies and Presidential directives into the unified national approach to implementing the CI/KR protection mission. The relevant authorities include those that address the overarching homeland security and CI/KR protection missions, as well as those that address a wide range of sector-specific CI/KR protection-related functions, programs, and responsibilities. This section describes how these overarching homeland security legislation, strategies, HSPDs, and related initiatives work together (see figure 5-1). Information regarding sector-specific CI/KR-related authorities will be addressed in the SSPs.

5.1.1 Legislation

The Homeland Security Act (figure 5-1, column 1) provides the primary authority for the overall homeland security mission and establishes the basis for the NIPP, the SSPs, and related CI/KR protection efforts and activities. A number of other statutes (as described in chapter 2 and appendix 2A) provide authorities for cross-sector and sector-specific CI/KR protection activities. SSPs will address relevant sector-specific authorities.

5.1.2 Strategies

The National Strategy for Homeland Security, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace together provide the vision and strategic direction for the CI/KR protection elements of the homeland security mission (see figure 5-1, columns 1 and 2). A number of other Presidential strategies, such as the National Intelligence Strategy, provide direction and guidance related to CI/KR protection on a national or sector-specific basis (see appendix 2A).

5.1.2.1 The National Strategy for Homeland Security

The President's National Strategy for Homeland Security established protection of America's CI/KR as a core homeland security mission and as a key element of the comprehensive approach to homeland security and domestic incident

management. This strategy articulated the vision for a unified "American Infrastructure Protection effort" to "ensure we address vulnerabilities that involve more than one infrastructure sector or require action by more than one agency," and to "assess threats and vulnerabilities comprehensively across all infrastructure sectors to ensure we reduce the overall risk to the country, instead of inadvertently shifting risk from one potential set of targets to another."

This strategy called for the development of "interconnected and complementary homeland security systems that are reinforcing rather than duplicative, and that ensure essential requirements are met … [and] provide a framework to align the resources of the Federal budget directly to the task of securing the homeland."

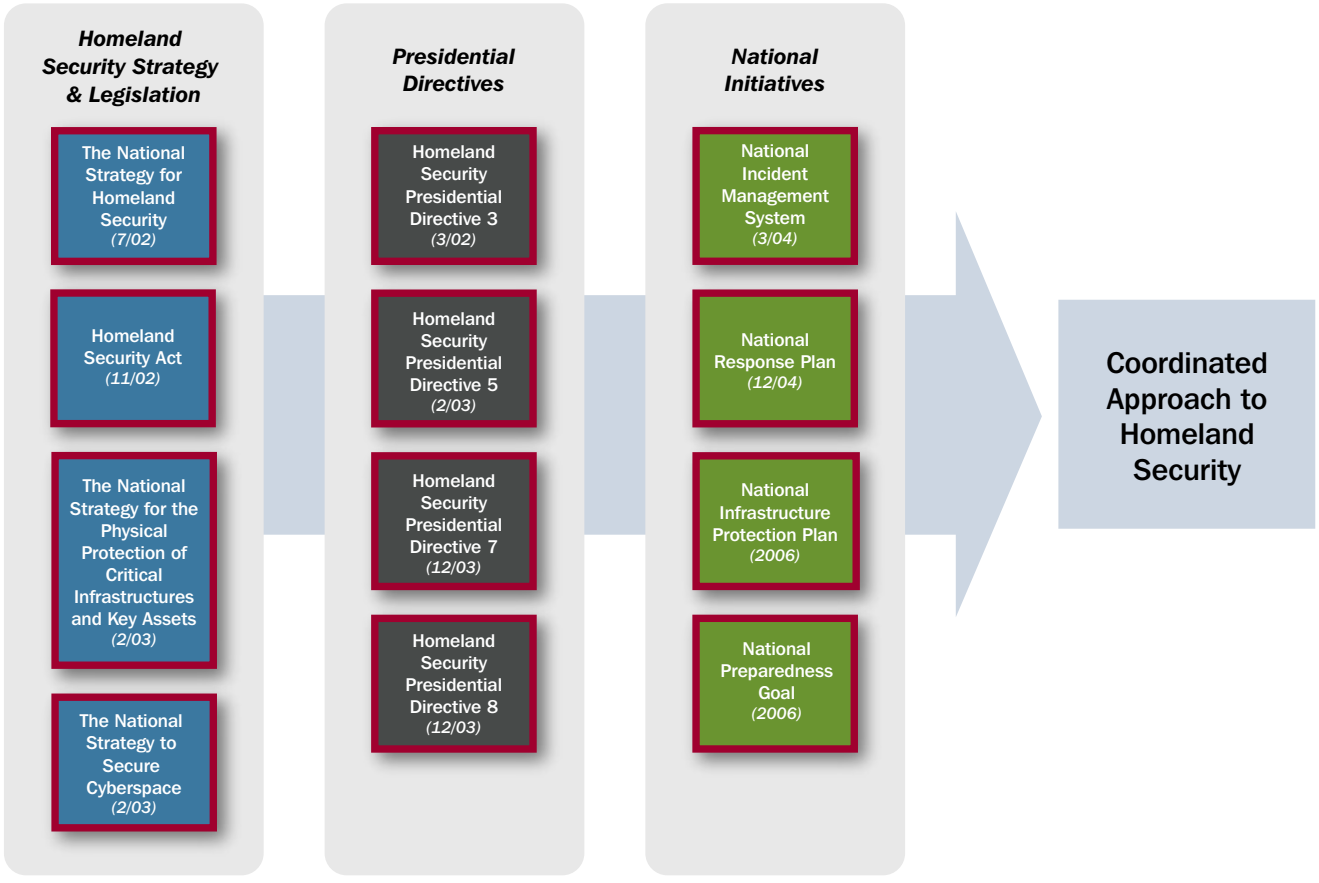
5.1.2.2 The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets identifies national policy, goals, objectives, and principles needed to "secure the infrastructures and assets vital to national security, governance, public health and safety, economy, and public confidence." The strategy identifies specific initiatives to drive near-term national protection priorities and inform the resource allocation process; identifies key initiatives needed to secure each of the CI/KR sectors; and addresses specific cross-sector security priorities. Additionally, it establishes a foundation for building and fostering the cooperative environment in which government, industry, and private citizens can carry out their respective protection responsibilities more effectively and efficiently.

5.1.2.3 The National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace sets forth objectives and specific actions needed to prevent cyber attacks against America's CI/KR; identifies and appropriately responds to those responsible for cyber attacks; reduces nationally identified vulnerabilities; and minimizes damage and recovery time from cyber attacks. This strategy articulates five national priorities, including the establishment of a security response system, a threat and vulnerability reduction

Figure 5-1: National Framework for Homeland Security



program, awareness and training programs, efforts to secure government cyberspace, and international cooperation.

Priority in this strategy is focused on improving the national response to cyber incidents; reducing threats from and vulnerabilities to cyber attacks; preventing cyber attacks that could affect national security assets; and improving the international management of and response to such attacks.

5.1.3 Homeland Security Presidential Directives and National Initiatives

Homeland Security Presidential directives set national policies and executive mandates for specific programs and activities (see figure 5-1, column 3). The first was issued on October 29, 2001, shortly after the attacks on September 11, 2001, establishing the Homeland Security Council. It was followed by a series of directives regarding the full spectrum of actions required to "prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from incidents that do occur." A number of these are relevant to CI/KR protection. HSPD-3, Homeland Security Advisory System, provides the requirement for the dissemination of information regarding terrorist acts to Federal, State, and local authorities, and the American people. HSPD-5 addresses the national approach to domestic incident management; HSPD-7 focuses on the CI/KR protection mission; and HSPD-8 focuses on ensuring the optimal level of preparedness to protect, prevent, respond to, and recover from terrorist attacks and the full range of natural and manmade hazards.

This section addresses the Homeland Security Presidential directives that are most relevant to the overarching CI/KR protection component of the homeland security mission (e.g., HSPDs 3, 5, 7, and 8). Other Presidential directives, such as HSPD-9, Defense of the United States Agriculture and Food, and HSPD-10, Biodefense for the 21st Century, are relevant to CI/KR protection in specific sectors and will be addressed in further detail in the appropriate SSPs.

5.1.3.1 HSPD-3, Homeland Security Advisory System

HSPD-3 (March 2002) established the policy for the creation of the HSAS to provide warnings to Federal, State, and local authorities, and the American people in the form of a set of graduated Threat Conditions that escalate as the risk of the threat increases. At each threat level, Federal departments and agencies are required to implement a corresponding set of protective measures to further reduce vulnerability or increase response capabilities during a period of heightened alert. The threat conditions also serve as guideposts for the implementation of tailored protective measures by State, local, tribal, and private sector security partners.

5.1.3.2 HSPD-5, Management of Domestic Incidents

HSPD-5 (February 2003) required DHS to lead a coordinated national effort with other Federal departments and agencies; State, local, and tribal governments; and the private sector to develop and implement a National Incident Management System (NIMS) and the NRP (see figure 5-1, column 4).

The NIMS (March 2004) provides a nationwide template enabling Federal, State, local, and tribal governments; the private sector; and nongovernmental organizations to work together effectively and efficiently to prevent, prepare for, respond to, and recover from incidents regardless of cause, size, and complexity. The NIMS provides a uniform doctrine for command and management, including Incident Command, Multiagency Coordination, and Joint Information Systems; resource, communications, and information management; and application of supporting technologies.

The NRP (December 2004) was built on the NIMS template, signed by 29 Federal departments and agencies and 3 nongovernmental organizations, and fully implemented on April 14, 2005. It establishes a single, comprehensive framework for the management of domestic incidents (including threats) that require DHS coordination and effective response by an appropriate combination of Federal, State, local, and tribal governments; the private sector; and nongovernmental organizations.

5.1.3.3 HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection

HSPD-7 (December 2003) established the U.S. policy for "enhancing protection of the Nation's CI/KR." It mandated development of the NIPP as the primary vehicle for implementing the CI/KR protection policy. HSPD-7 directed the Secretary of Homeland Security to lead development of the plan, including, but not limited to, the following four key elements:

- A strategy to identify and coordinate the protection of CI/KR;
- A summary of activities to be undertaken to prioritize, reduce the vulnerability of, and coordinate protection of CI/KR;
- A summary of initiatives for sharing information and for providing threat and warning data to State, local, and tribal governments and the private sector; and

- Coordination and integration, as appropriate, with other Federal emergency management and preparedness activities, including the NRP and guidance provided in the National Preparedness Goal.

HSPD-7 also directed the Secretary of Homeland Security to maintain an organization to serve as a focal point for the security of cyberspace. The NIPP is supported by a series of SSPs, developed by the SSAs in coordination with their public and private sector security partners, which detail the approach to CI/KR protection goals, initiatives, processes, and requirements for each sector.

5.1.3.4 HSPD-8, National Preparedness

HSPD-8 (December 2003) mandates development of a National Preparedness Goal (see figure 5-1, column 4) aimed at helping entities at all levels of government build and maintain the capabilities to prevent, protect against, respond to, and recover from major events "to minimize the impact on lives, property, and the economy."

To do this, the National Preparedness Goal provides readiness targets, priorities, standards for assessments and strategies, and a system for assessing the Nation's overall level of preparedness across four mission areas: prevention, protection, response, and recovery. The goal currently specifies three overarching priorities: (1) implementation of the NIMS and the NRP; (2) expansion of regional collaboration; and (3) implementation of the NIPP and several capability-specific priorities, which include strengthening information-sharing and collaborative capabilities; interoperable communications capabilities; and chemical, biological, radiological, nuclear, or explosive detection, response, and decontamination. The national priorities establish "measurable readiness priorities … that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them." Each of these priorities is relevant to enhancing effective implementation of the NIPP and integration of the NIPP risk management framework as a vital component of achieving the Nation's homeland security mission. With progress toward fulfillment of these priorities and continuous learning, identification of additional priorities is anticipated.

The National Preparedness Goal uses capabilities-based planning processes and enables Federal, State, local, and tribal entities to prioritize needs, update strategies, allocate resources, and deliver programs. The goal references standard planning tools that are applicable to implementation of the NIPP, including the UTL and the TCL. The UTL provides a menu of tasks from all sources that may be performed to implement CI/KR protection programs, as well as those needed to respond to major incidents. The TCL provides guidance on the specific capabilities and levels of capability relevant to CI/KR protection and other areas of the homeland security mission that Federal, State, local, and tribal entities will be expected to develop and maintain. These will vary based on the risk and the needs of the various entities involved. Like the NIPP, the UTL and TCL are living documents that will be enhanced and refined over time.

5.2 The CI/KR Protection Component of the Homeland Security Mission

The result of this interrelated set of national authorities, strategies, and initiatives is a common, holistic approach to achieving the homeland security mission that includes an emphasis on preparedness across the board, and on the protection of America's CI/KR as a steady-state component of routine, day-to-day business operations for government and private sector security partners.

The NIPP and NRP are complementary plans that span a spectrum of prevention, protection, response, and recovery activities to enable this coordinated approach on a day-to-day basis, as well as during periods of heightened threat. The NIPP and its associated SSPs establish the Nation's steady-state level of protection by helping to focus resources where investment yields the greatest return in terms of national risk management. The NRP addresses prevention, preparedness, response, and recovery in the context of domestic threat and incident management. The National Preparedness Goal supports implementation of both the NIPP and the NRP by establishing national priorities and guidance for building the requisite capabilities to support both plans at all levels of government.

Each of the guiding elements of the homeland security mission includes specific requirements for DHS and other Federal departments and agencies to build partnerships and work in cooperation and collaboration with State, local, tribal, and private sector partners. This cooperation and collaboration between government and private sector owners and operators is specifically applicable to the CI/KR protection efforts outlined in the NIPP.

The NIPP risk management framework, sector partnership model, and information-sharing mechanisms are structured to support coordination and cooperation with private sector owners and operators while recognizing the differences between and within sectors, acknowledging the need to protect sensitive information, establishing processes for

information sharing, and providing for smooth transitions from steady-state operations to incident response.

5.3 Relationship of the NIPP and SSPs to Other CI/KR Plans and Programs

The NIPP Base Plan, Appendixes, and SSPs outline the overarching elements of the CI/KR protection effort that generally are applicable within and across all sectors. The SSPs are an integral component of the NIPP and exist as independent documents to address the unique perspective, risk landscape, and methodologies associated with each sector. Homeland security plans and strategies at the State, local, and tribal levels of government address CI/KR protection within their respective jurisdictions, as well as mechanisms for coordination with various regional efforts and other external entities. The NIPP also is designed to work with the range of CI/KR protection-related plans and programs instituted by the private sector, both through voluntary actions and as a result of various regulatory requirements. These plans and programs include business continuity and resilience measures. NIPP processes are designed to enhance coordination, cooperation, and collaboration among security partners within and across sectors to synchronize related efforts and avoid duplicative or unnecessarily costly security requirements.

5.3.1 Sector-Specific Plans

Based on guidance from DHS, SSPs are developed jointly by SSAs in close collaboration with SCCs, GCCs, and others, including State, local, and tribal homeland security partners with key interests or expertise appropriate to the sector. The SSPs provide the means by which the NIPP is implemented across all sectors, as well as a national framework for each sector that guides the development, implementation, and updating of State and local homeland security strategies and CI/KR protection programs. Generally, SSPs will be unclassified; some SSPs or portions of SSPs containing sensitive information may be classified and subject to more stringent document control and limited distribution to security partners with appropriate clearances and a need to know.

SSPs are tailored to address the unique characteristics and risk landscapes of each sector while also providing consistency for protective programs, public and private protection investments, and resources. SSPs serve to:

- Define sector security partners, authorities, regulatory bases, roles and responsibilities, and interdependencies;
- Establish or institutionalize already existing procedures for sector interaction, information sharing, coordination, and partnership;
- Establish the goals and objectives, developed collaboratively between security partners, required to achieve the desired protective posture for the sector;
- Identify international considerations;
- Identify areas for government action above and beyond an owner/operator or sector risk model; and
- Identify the sector-specific approach or methodology that SSAs, in coordination with DHS and other security partners, will use to conduct the following activities consistent with the NIPP framework:
  - Identify priority CI/KR and functions within the sector, including cyber considerations;
  - Assess sector risks, including potential consequences, vulnerabilities, and threats;
  - Assess and prioritize assets, systems, networks, and functions of national-level significance within the sector;
  - Develop risk-mitigation programs based on detailed knowledge of sector operations and risk landscape;
  - Provide protocols to transition between steady-state CI/KR protection and incident response in an all-hazards environment;
  - Use metrics to measure and communicate program effectiveness and risk management within the sector;

Figure 5-2: Sector-Specific Plan Structure

– Address R&D requirements and activities relevant to the sector; and

– Identify the process used to promote governance and information sharing within the sector.

The structure for the SSPs is shown in figure 5-2; it facilitates cross-sector comparisons and coordination by DHS and other SSAs.

The SSPs must be completed and submitted by the SSAs to DHS within 180 days of issuance of the NIPP. The SSP concurrence process includes a formal review process for GCC member departments and agencies, as well as demonstrated/documented collaboration and coordination with the SCC, which may include letters of endorsement or statements of concurrence.

5.3.2 State, Regional, Local, and Tribal CI/KR Protection Programs

The National Preparedness Goal defines the development and implementation of a CI/KR protection program as a key component of State, regional, local, and tribal homeland security programs. Creating and managing a CI/KR protection program for a given jurisdiction entails building an organizational structure and mechanisms for coordination between government and private sector entities that can be used to implement the NIPP risk management framework. This includes taking actions within the jurisdiction to set security goals; identifying assets, systems, and networks; assessing risks; prioritizing CI/KR across sectors and jurisdictional levels; implementing protective programs; measuring the effectiveness of risk management efforts; and sharing information between relevant public and private sector security partners. These elements form the basis of focused CI/KR protection programs and guide the implementation of the relevant CI/KR protection-related goals and objectives outlined in State, local, and tribal homeland security strategies.

In a regional context, the NIPP risk management framework and information-sharing processes can be applied through the development of a regional partnership model or the use of existing regional coordinating structures. Effective regional approaches to CI/KR protection involve coordinated information sharing, planning, and sharing of costs and risk. Regional approaches also include exercises to bring public and private sector partners together around a shared understanding of the challenges to regional resilience; analytical tools to inform decisionmakers on risk and risk management with the associated benefits and costs; and forums to enable decisionmakers to formulate protective measures and identify funding requirements and resources within and across sectors and jurisdictions.

State, regional, local, and tribal CI/KR protection efforts enhance implementation of the NIPP and the SSPs by providing unique geographical focus and cross-sector coordination potential. To ensure that these efforts are consistent with other CI/KR protection planning activities, the basic elements to be incorporated in these efforts are provided in appendix 5A. The recommended elements described in this appendix recognize the variations in governance models across the States; recognize that not all sectors are represented in each State or geographical region; and are flexible enough to reflect varying authorities, resources, and issues within each State or region.

5.3.3 Other Security Partner Plans or Programs Related to CI/KR Protection

Federal security partners should review and revise, as necessary, other plans that address elements of CI/KR protection to ensure that they support the NIPP in a manner that avoids unnecessary layers of CI/KR protection guidance. Examples of government plans or programs that may contain relevant prevention, protection, and response activities that relate to or affect CI/KR protection include plans that address: State, local, and tribal hazard mitigation; continuity of operations; continuity of government; environmental, health, and safety operations; and integrated contingency operations. Federal security partners are required to complete the review of existing plans within 90 days and complete any required revisions within 180 days of the issuance of the NIPP. Review and revision of State, local, and tribal strategies and plans should be completed in accordance with overall homeland security and grant program guidance.

Private sector owners and operators develop and maintain plans for business risk management that include steady-state security and facility protection, as well as business continuity and emergency management plans. Many of these plans include heightened security requirements for CI/KR protection that address the terrorist threat environment. Coordination with these planning efforts is relevant to effective implementation of the NIPP. Private sector security partners are encouraged to consider the NIPP when revising these plans, and to work with government security partners to integrate their efforts with Federal, State, local, and tribal CI/KR protection efforts as appropriate.

5.4 CI/KR Protection and Incident Management

Together, the NIPP and the NRP provide a comprehensive, integrated approach to addressing key elements of the Nation's homeland security mission to prevent terrorist attacks, reduce vulnerabilities, and respond to incidents in an all-hazards context. The NIPP establishes the overall risk-based approach that defines the Nation's CI/KR steady-state protective posture, while the NRP and NIMS provide the overarching framework, mechanisms, and protocols required for effective and efficient domestic incident management. The NIPP risk management framework, information-sharing network, and sector partnership model provide vital functions that, in turn, inform and enable incident management decisions and activities.

5.4.1 The National Response Plan

The NRP provides an all-hazards approach that incorporates best practices from a wide variety of disciplines, including fire, rescue, emergency management, law enforcement, public works, and emergency medical services. The operational and resource coordinating structures described in the NRP are designed to support decisionmaking during the response to a specific threat or incident and serve to unify and enhance the incident management capabilities and resources of individual agencies and organizations acting under their own authority. The NRP applies to a wide array of natural disasters, terrorist threats and incidents, and other emergencies.

The NRP Base Plan and annexes provide protocols for coordination among various Federal departments and agencies; State, local, and tribal governments; and private sector partners, both for pre-incident prevention and preparedness, and post-incident response, recovery, and mitigation. The NRP specifies incident management roles and responsibilities, including emergency support functions designed to expedite the flow of resources and program support to the incident area. SSAs and other Federal departments and agencies have roles within the NRP structure that are distinct from, yet complementary to, their responsibilities under the NIPP. Ongoing implementation of the NIPP risk management framework, partnerships, and information-sharing networks sets the stage for CI/KR security and restoration activities within the NRP framework by providing mechanisms to quickly assess the impacts of the incident on both local and national CI/KR, assist in establishing priorities for CI/KR restoration, and augment incident-related information sharing with security partners.

5.4.2 Transitioning From NIPP Steady-State to Incident Management

A variety of alert and warning systems that exist for natural hazards, technological or industrial accidents, and terrorist incidents provide the bridge between routine steady-state operations using the NIPP risk management framework and incident management activities using the NRP concept of operations for actions related to both pre-incident prevention and post-incident response and recovery. These all-hazards alert and warning mechanisms include programs such as National Weather Services hurricane and tornado warnings, and alert and warning systems established around nuclear power plants and chemical stockpiles, among various others. In the context of terrorist incidents, the HSAS provides a progressive and systematic approach that is used to match protective measures to the Nation's overall threat environment. This link between the current threat environment and the corresponding protective actions related to specific threat vectors or scenarios and to each HSAS threat level provides the indicators used to transition from the steady-state processes detailed in the NIPP to the incident management processes described in the NRP.

DHS and security partners develop and implement stepped-up, protective actions to match the increased terrorist threat conditions specified by the HSAS, and to address various other all-hazards alerts and warning requirements. As warnings or threat levels increase, NRP coordinating structures are activated to enable incident management. DHS and security partners carry out their NRP responsibilities and also use the NIPP risk management framework to provide the CI/KR protection dimension needed to inform NRP incident command and control, and multi-agency coordination. When an incident occurs, regardless of the cause, the NRP is implemented for overall coordination of domestic incident management activities. The NIPP provides the CI/KR dimension, reinforcing NRP incident management coordinating structures and processes. Implementation of the NIPP risk management framework facilitates those actions directly related to the current threat status, as well as incident prevention, response, restoration, and recovery.

The process for integrating CI/KR protection with incident management and transitioning from NIPP steady-state processes to NRP incident management coordination includes the following actions by DHS, SSAs, and other security partners:

- Increasing protection levels to correlate with the specific threat vectors or threat level communicated through the HSAS or other relevant all-hazards alert and warning

systems, or in accordance with sector-specific warnings using the NIPP information-sharing networks;

- Using the NIPP information-sharing networks and risk management framework to review and establish national priorities for CI/KR protection; facilitating communications between security partners; and informing the NRP processes regarding priorities for response, recovery, and restoration of CI/KR within the incident area, as well as on a national scale;
- Fulfilling roles and responsibilities as defined in the NRP for incident management activities; and
- Working with sector-level information-sharing entities and owners and operators on information-sharing issues during the active response mode.

6. Ensuring an Effective, Efficient Program Over the Long Term

This chapter addresses the efforts needed to ensure an effective, efficient CI/KR protection program over the long term. It focuses particularly on the long-lead-time elements of CI/KR protection that require sustained plans and investments over time, such as generating skilled human capital, developing high-tech systems, and building public awareness.

Key activities needed to enhance CI/KR protection over the long term include:

- **Building national awareness** to support the CI/KR protection program, related protection investments, and protection activities by ensuring a focused understanding of the all-hazards threat environment and of what is being done to protect and enable the timely restoration of the Nation's CI/KR in light of such threats;
- **Enabling education, training, and exercise programs** to ensure that skilled and knowledgeable professionals and experienced organizations are able to undertake NIPP-related responsibilities in the future;
- **Conducting R&D and using technology** to improve protective capabilities or to lower the costs of existing capabilities so that security partners can afford to do more with limited budgets;
- **Developing, protecting, and maintaining data systems and simulations** to enable continuously refined risk assessment within and across sectors and to ensure preparedness for domestic incident management; and
- **Continuously improving the NIPP** and associated plans and programs through ongoing management and revision, as required.

6.1 Building National Awareness

The development and implementation of a national awareness program for CI/KR protection was identified as a major need in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. DHS, in conjunction with the SSAs and other security partners, is responsible for developing and implementing a comprehensive national awareness program that supports the sustainability of CI/KR protection, security investments, and focused public and private sector understanding of the CI/KR all-hazards risk environment.

The objectives of the national awareness program are to:

- Incorporate CI/KR protection and restoration considerations into business planning and operations, including employee and senior manager education and training programs, across all levels of government and the private sector;

- Support public and private sector decisionmaking and enable the planning of relevant and effective protection and restoration strategies and inform resource allocation processes;
- Develop an understanding of CI/KR dependencies and interdependencies and the value of cross-sector CI/KR protection and restoration planning down to the community level;
- Maintain public understanding of the evolving threat to CI/KR as assessed by the intelligence community and in the context of the HSAS; and
- Build public understanding of efforts to address the threat environment and enhance protection and rapid restoration of the Nation's CI/KR.

DHS and other Federal agencies are also engaged in a comprehensive national cyberspace security awareness campaign to remove impediments to sharing vulnerability information among security partners. This campaign includes audience-specific awareness materials, expansion of the Stay Safe Online campaign, and development of awards programs for those in industry who make significant contributions to the effort.

6.2 Enabling Education, Training, and Exercise Programs

The NIPP establishes a framework to enable the education, training, and exercise programs that allow people and organizations to develop and maintain key CI/KR protection expertise. Building the requisite individual and organizational expertise requires attracting, training, and maintaining sufficient numbers of professionals who have the particular expertise unique or essential to CI/KR protection. This, in turn, requires *individual* education and training to develop and maintain the requisite levels of expertise through technical, academic, and professional development programs. It also requires *organizational training and exercises* to develop the requisite organizational-level expertise. The framework that the NIPP establishes to enable each of these is discussed below.

6.2.1 Types of Expertise for CI/KR Protection

Some types of CI/KR protection expertise are associated with well-established disciplines that already feature formal academic education programs, recognized technical training levels and credentials, and professional certification systems implemented through professional organizations or government licensing. Others involve unique skills and professional expertise that are specific to CI/KR protection, such as the expertise needed to implement the NIPP risk management framework. Such expertise often involves cutting-edge approaches that are not yet widely practiced and have yet to develop academic degrees or professional certification mechanisms in a nationwide system. The NIPP focuses special emphasis on the types of expertise that are unique to or essential for CI/KR protection. These include:

- Risk assessment and risk management and related concepts used in business continuity planning;
- Cost-benefit analysis to inform risk management priorities;
- Resource allocation based on risk management priorities;
- Analysis of insider threats to CI/KR and applicable countermeasures;
- Analysis of physical and cyber threats to CI/KR, including control systems, and cyber security measures;
- CI/KR dependency and interdependency analyses;
- International aspects of CI/KR protection;
- Best practices and technical capabilities for CI/KR protection, business continuity, and resiliency; and
- Best practices and technical capabilities for information sharing and protection.

6.2.2 Individual Education and Training

The NIPP recognizes the importance of leveraging existing accredited academic programs, professional certification standards, and technical training programs that are in place for the more mature and established disciplines. Whether CI/KR protection disciplines are established or newly evolving, they must include the technical, academic, and professional skill sets upon which the NIPP and SSPs are based. This requires an effort with a national scope that includes, but is not limited to, the following components:

- Technical training to provide individuals with the skills needed to perform their roles and responsibilities under the NIPP;
- Academic and research programs that result in formal degrees from accredited institutions; and
- Professional continuing education, which incorporates the latest advances in CI/KR risk-mitigation approaches and,

where appropriate, certification based on government, industry, and professional organization standards.

To enable each of these components, the NIPP specifies areas of emphasis that are discussed in the subsections that follow.

6.2.2.1 Technical CI/KR Protection Training

Training that is technical in nature can be grouped into two major categories: (1) specific technical training on the details of the NIPP itself for staff and decisionmakers, and (2) broader operational training for those charged with implementing CI/KR protection programs or who work in a CI/KR facility or operate a critical system or network. Each are described below:

- **Specialized NIPP Training:** Training for managers and staff responsible for NIPP implementation should provide an awareness level of training on all aspects of the NIPP, including, but not limited to, the underlying authorities; responsibilities; risk management framework; sector partnership model; information sharing; protection program requirements; and planning, resource, and budget processes. The basic awareness-level training should also provide participants with a working knowledge of how to use the NIPP and apply its principles and processes, both for steady-state CI/KR protection and to enable the CI/KR protection dimension of domestic incident management.

  DHS will provide or coordinate the development of course materials on these topics; work with security partners, SCCs, and GCCs to facilitate the definition of general training requirements; and guide the development of national-level training standards associated with the NIPP. DHS will facilitate initial training in these topics for security partners, as appropriate.

- **Operational CI/KR Protection Training:** Technical CI/KR protection training programs for security partners enhance the knowledge and skills required to detect, deter, defend, and mitigate against terrorist activities and other incidents and events that threaten CI/KR. DHS and other Federal agencies support and provide training resources to local law enforcement officers and others, with a special focus on urban areas with significant clusters of CI/KR, localities where high-profile special events are typically scheduled, or other potentially high-risk geographical areas or jurisdictions. Federally provided technical training courses cover a range of operational and technical topics, such as buffer zone protection, bombing prevention, workforce terrorism awareness, surveillance detection, high-risk target awareness, and WMD incident training.

DHS also supports cyber security training, education, and awareness programs by educating vendors and manufacturers on the value of pre-configuring security options in products so that they are secure on initial installation; educating users on secure installation and use of cyber products; increasing user awareness and ease of use of the security features in products; and, where feasible, promotion of industry guides. These training efforts also encourage programs that leverage the existing Cyber Corps Scholarship for Service program, as well as various graduate and post-doctoral programs; link Federal cyber security and computer forensics training programs; and establish cyber security programs for departments and agencies, including awareness, audits, and standards as required.

Other Federal agencies also offer training related to CI/KR protection. For example, the Office of Personnel Management and DOD offer courses on CI/KR target awareness and best practices risk-mitigation measures. The Department of the Treasury also works with DHS to jointly provide training for criminal investigators in basic computer forensics.

DHS solicits recommendations from national professional organizations and from Federal, State, local, tribal, and private sector security partners for additional discipline-specific technical training courses related to CI/KR protection, and supports course development as appropriate.

6.2.2.2 Academic and Research Programs

DHS works with a wide range of academic institutions to incorporate CI/KR protection into professional education programs. For example, DHS collaborates with universities to incorporate a security-related curriculum into business school programs under Project MBA (master's of business administration) to better prepare the Nation's future business leaders to plan, implement, and manage CI/KR protection programs. DHS also sponsors a post-graduate-level program at the Naval Postgraduate School in homeland defense and security.

DHS will examine existing cyber security programs within the research and academic communities to determine their applicability as models for CI/KR protection education and broad-based research. These programs include:

- Co-sponsorship of the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) program with the National Security Agency (NSA); and
- Collaboration with the National Science Foundation to co-sponsor the Cyber Corps Scholarship for Service program. The Scholarship for Service program provides grant money

to selected CAEIAE and other universities with programs of a similar caliber to fund the final 2 years of student bachelor's, master's, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal Government.

DHS will ensure that the NCIP R&D Plan appropriately considers the human capital needs for protection-related R&D by incorporating analysis of the research community's future needs for advanced degrees in protection-related disciplines into the plan development process.

6.2.2.3 Continuing Education and Professional Competency

CI/KR protection involves many skills and professions that already feature education, training, and certification programs through professional organizations or government licensing. The CI/KR protection field also involves unique skills and professional expertise that have yet to incorporate such training and certification mechanisms into a nationwide system.

DHS encourages and, when appropriate, works with security partners to facilitate the development of continuing education, professional competency programs, and professional standards for areas requiring unique and critical CI/KR protection expertise. For example, DHS is collaborating with DOD to guide the development of a national certification program that includes a comprehensive set of information technology job skill standards for security professionals within the Federal Government and private industry. DHS will encourage and, when appropriate, facilitate the development of similar professional and surety standards for the remaining areas of unique and critical CI/KR protection expertise specified above.

6.2.3 Organizational Training and Exercises

Building and maintaining organizational and sector expertise requires comprehensive exercises to test the interaction between the NIPP and the NRP in the context of terrorist incidents, natural disasters, and other emergencies. Exercises are conducted by private sector owners and operators, and across all levels of government; they may be organized by these entities, on a sector-specific basis, or through three major national-level programs:

- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP and their transition to the incident management framework established in the NRP. Some examples of national exercises include TOPOFF and Ardent Sentry.
- **Homeland Security Exercises and Evaluation Program:** DHS also provides policy and guidance for designing, developing, conducting, and evaluating exercises to its security partners. HSEEP is a threat- and performance-based exercise program that includes a mix and range of exercise activities of varying degrees of complexity and interaction. HSEEP also includes a series of four reference manuals to help States and local jurisdictions establish exercise programs and design, develop, conduct, and evaluate exercises.
- **National Cyber Exercises:** DHS conducts exercises to identify, test, and improve coordination within the cyber incident response community, including Federal, State, local, tribal, and international government elements, as well as private sector corporations and coordinating councils. The Cyber Storm exercise conducted in February 2006 is an example of a national cyber exercise event.

DHS and the SSAs work together to ensure that these exercises include adequate testing of steady-state CI/KR protection

Pursuant to the National Exercise Plan, the **DHS Top Officials (TOPOFF)** national exercise series is a congressionally mandated, interagency program designed to strengthen the Nation's capacity to prevent, protect against, respond to, and recover from terrorist attacks involving WMD. This biennial exercise series is the cornerstone of the DHS National Exercise Program.

Ardent Sentry is an annual terrorism exercise focused on defense support to civil authorities that is jointly sponsored by the North American Aerospace Defense Command (NORAD) and the U.S. Northern Command (NORTHCOM). Ardent Sentry has been integrated with the DHS National Homeland Security Exercise Program and may be held concurrently with the TOPOFF exercises.

The **National Cyber Exercise** series is sponsored by the DHS National Cyber Security Division to strengthen preparedness, response, coordination, and recovery mechanisms to cyber incidents within international, Federal, and State governments, and in conjunction with the private sector. In accordance with congressional mandates to conduct exercises that test response to cyber attacks on critical infrastructures, the exercise meets HSPD-8, National Preparedness, requirements and is coordinated with the DHS National Exercise Program.

measures and plans, including information sharing; application of the NIPP risk management framework; and the ability for a protected core of life-critical CI/KR services, such as power, food and water, and emergency transportation, to withstand attacks or natural disasters and continue to function at an appropriate level.

DHS works with other security partners to facilitate the development of national standards, guidelines, and protocols for incident management training and exercises that include CI/KR protection evaluation to ensure that exercise programs include adequate testing of CI/KR steady-state protective measures and incident plans.

DHS will ensure that the NIMS Integration Center, which serves as the repository and clearinghouse for reports and lessons learned from actual incidents, training, and exercises, regularly compiles and disseminates information on CI/KR protection best practices.

6.2.4 Security Partner Role and Approach

Given the scope and nature of the education, training, and exercise needs related to CI/KR protection, the approach adopted must, to the greatest extent possible, leverage existing education, training, and exercise programs.

DHS will work through the NIPP partnership structure to provide initial training on the NIPP to introduce key public and private sector security partners to the plan's contents and requirements. DHS also will encourage and, where appropriate, facilitate specialized NIPP training, professional training, continuing education, and development of professional and personnel surety guidelines. It also will encourage academic and research programs, and coordinate with exercise managers on the design of exercises that test the interaction between the NIPP framework and the NRP.

The Interagency CI/KR Protection Training Task Force defines general training requirements and guides the development of national-level training standards associated with the NIPP. The SSAs and other Federal agencies should review and update existing CI/KR protection-related courses to align with the NIPP. Other security partners are encouraged to review existing courses to align with the NIPP or develop courses relevant to CI/KR protection needs within their jurisdiction. All security partners should work with DHS and the SSAs to identify and fill gaps in current training, education, and exercise programs for those specialized disciplines that are unique to CI/KR protection.

6.3 Conducting Research and Development and Using Technology

Federal agencies conduct R&D programs to help develop knowledge and technology that can be used by security partners to more effectively mitigate the risk to CI/KR. Congress has provided for liability protections under the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) that serve to encourage technology use by CI/KR security partners.

6.3.1 R&D Programs

In the near term, risk-based priorities are designed to address the challenges posed by the limited resources available to meet all CI/KR protection needs by allocating protection resources where they can best mitigate risk. In the long term, R&D holds the key to more effective and cost-efficient CI/KR protection through advances in technology. R&D programs work to improve all aspects of CI/KR protection—from detection of threats, through protection and performance measures, to inherently secure advanced infrastructure designs. Because owners and operators play a major role in CI/KR protection, research programs that support the NIPP must find effective ways to consider the perspectives of sector professional associations, sector councils, and other sources that understand owner and operator technology needs.

Unique R&D needs associated with CI/KR protection include:

- Conducting development, or re-design, of technology-based equipment to significantly lower the costs of existing capabilities rather than improving technical performance, so that security partners with limited budgets can afford state-of-the-art solutions;
- Researching issues, such as resiliency and protection in building design, that affect all CI/KR and can result in solutions that can provide benefits across sectors if implemented; and
- Focusing research on the implementation and operational aspects of technology used for CI/KR protection to provide resources that can help inform technology investment decisions, such as technical evaluation of security equipment or technology clearing house information.

R&D supporting the NIPP includes planning and program activities undertaken in three general areas: (1) the NCIP R&D Plan, (2) the Federal Plan for Cyber Security R&D, and (3) R&D and planning efforts conducted by the SSAs and other agencies in support of the requirements set forth in the President's Physical and Cyber CI/KR Protection Strategies.

Additionally, Technology Pilot Programs are used to develop solutions to CI/KR protection problems with technologies that have passed the research stage and require demonstration in operational use. Each of these is discussed in the sections that follow. Appendix 6 provides more details on specific R&D plans and programs supporting CI/KR protection.

6.3.2 The SAFETY Act

As part of the Homeland Security Act, Public Law 107-296, Congress enacted the SAFETY Act, which creates liability protections for sellers of qualified anti-terrorism technologies. The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by limiting liability through a system of risk and litigation management. The purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential sellers of anti-terrorism technologies from developing, deploying, and commercializing technologies that could save lives. The SAFETY Act gives liability protection to both sellers of qualified anti-terrorism technology and their customers, and applies to all types of enterprises that develop, sell, or use anti-terrorism technologies.

The SAFETY Act applies to a broad range of technologies, including products, services, and software, or combinations thereof, as well as technology firms and providers of security services. The SAFETY Act protects those businesses and their customers and contractors by providing a series of liability protections if their products or services are found to be effective by the Secretary of Homeland Security. Additionally, if the Secretary certifies the technology under the SAFETY Act (i.e., that the technology actually performs as it is intended to do and/or conforms to certain seller specifications), the seller is afforded a complete defense in litigation related to the performance of the technology in preventing, detecting, or deterring terrorist acts or deployment to recover from one. Those technologies that have been "certified" are placed on an Approved Product List for Homeland Security that is published at www.safetyact.gov.

A clear benefit of the SAFETY Act is that a cause of action may be brought only against the seller of the Qualified Anti-Terrorism Technology and may not be brought against the buyer(s), their contractors, or downstream users of the Qualified Anti-Terrorism Technology, or against the seller's suppliers or contractors. This stipulation includes CI/KR owners and operators.

CI/KR facility owners and operators are encouraged to examine the SAFETY Act closely because: (1) CI/KR owners (if purchasers of qualified technologies) will enjoy the liability protections that flow from using qualified SAFETY Act technologies, and (2) CI/KR owners will also have a level of assurance that the qualified products/services they are utilizing have been vetted by DHS. Lower liability insurance burdens for those using qualified technologies are another potential outcome.

In these ways, the SAFETY Act is a valuable tool that can enhance the ability of owners and operators to protect our Nation's CI/KR.

6.3.3 National Critical Infrastructure Protection R&D Plan

As directed by HSPD-7, the Secretary of Homeland Security works with the Director of the OSTP, Executive Office of the President, to develop the NCIP R&D Plan as a vehicle to support implementation of CI/KR risk management and supporting protective activities and programs.

The NCIP R&D Plan provides the focus and coordination mechanisms required to achieve the vision provided in the President's Physical and Cyber CI/KR Protection Strategies. That vision calls for a "systematic national effort to fully harness the Nation's research and development capabilities." The R&D planning process is designed to address common issues faced by the various sector security partners and ensure a coordinated R&D program that yields the greatest value across a broad range of interests and requirements. The plan addresses both physical and cyber CI/KR protection. The planning process also provides for the revision of research goals and priorities over the long term to respond to changes in the threat, technology, environment, business continuity, and other factors.

DHS and OSTP coordinate with Federal and private sector security partners, including academic and national laboratory representatives, during the R&D planning cycle. The interagency process used to develop and coordinate this plan is managed through the Infrastructure Subcommittee of the National Science and Technology Council (NSTC), which is co-chaired by DHS and OSTP. The SSAs are responsible for providing input into the plan after coordination with sector representatives and experts through such bodies as the SCCs and GCCs.

The NCIP R&D Plan articulates strategic R&D goals and identifies the R&D areas in which advances in CI/KR protection must be made. The plan also provides an R&D technology roadmap against which current and planned risk management and CI/KR protection R&D initiatives can be evaluated to define a program of CI/KR protection-related technology

development. The goals, R&D areas, and technology roadmap contained in the NCIP R&D Plan are discussed in the following subsections. A final subsection describes coordination of SSP R&D planning with the NCIP R&D Plan.

6.3.3.1 CI/KR Protection R&D Strategic Goals

The NCIP R&D planning process identifies three long-term, strategic R&D goals for CI/KR protection:

- A common operating picture architecture;
- A next-generation Internet architecture with designed-in security; and
- Resilient, self-diagnosing, self-healing systems.

The strategic goals are used to guide Federal R&D investment decisions and also to provide a coordinated approach to the overall Federal research program. The DHS Science and Technology (S&T) Directorate and OSTP will work with the OMB to use the R&D Plan as a decisionmaking tool for evaluation of budget submissions across Federal agencies. These goals also help guide programs of research performers who receive Federal grants and contracts.

6.3.3.2 CI/KR Protection R&D Areas

R&D development projects for CI/KR protection programs fall into nine R&D areas or themes that cut across all CI/KR sectors:

- Detection and sensor systems;
- Protection and prevention systems;
- Entry and access portals;
- Insider threats;
- Analysis and decision support systems;
- Response, recovery, and reconstitution tools;
- New and emerging threats and vulnerabilities;
- Advanced infrastructure architectures and systems design; and
- Human and social issues.

Organizing research in these areas enables the development of effective solutions that may be applied across sectors and disciplines. These themes also provide an organizing framework for SSA use during the development of R&D requirements for their respective sectors, which will be reflected in the SSPs. These requirements specify the capabilities each sector needs to satisfy CI/KR protection needs. By incorporating these requirements into the NCIP R&D Plan, OMB is better able to ensure that agency R&D budget requests are aligned with the National R&D Plan for CI/KR Protection.

6.3.3.3 CI/KR Protection R&D Roadmap

The NCIP R&D technology roadmap provides a way for Federal R&D managers such as DHS, OSTP, OMB, and the SSAs, to coordinate CI/KR protection R&D across NIPP security partners. This roadmap provides a systematic approach to identify current technology investment plans, determine gaps, and outline the timeline for addressing unmet requirements. It also provides a systematic way to determine interrelationships among other R&D programs, both public and private, and ensures synchronization with the SSA R&D plans contained in the SSPs.

6.3.3.4 Coordination of NCIP R&D Plan With SSP R&D Planning

Each SSP will include a component on sector-specific CI/KR protection R&D that explains how the sector will strengthen the linkage between sector-specific and national R&D planning efforts, technology requirements, current R&D initiatives, gaps, and candidate R&D initiatives. This component of the SSP explains the process for:

- **Sector Technology Requirements:** Identifying and providing a summary of sector technology requirements, and communicating them to the DHS S&T Directorate/OSTP for inclusion in the NCIP R&D Plan on an annual basis;
- **Current R&D Initiatives:** Annually soliciting a listing of current Federal R&D initiatives from the DHS S&T Directorate/OSTP that have the potential to meet sector CI/KR protection challenges, and providing a description of how this listing will be analyzed to indicate which initiatives have the greatest potential for a positive impact;
- **Gaps:** Conducting an analysis of the gaps between the sector's technology needs and current R&D initiatives from the DHS S&T Directorate/OSTP; and
- **Candidate R&D Initiatives:** Determining which candidate R&D initiatives are most relevant for the sector and how these will be summarized and reported to all appropriate stakeholders.

Each SSA will coordinate the development of the sector R&D planning component of their SSP so that these documents reflect the SSA's sector-level R&D investment priorities. Coordination between DHS/S&T and the sectors through the SSAs, GCCs, and SCCs ensures that the R&D information in the SSP will be consistently documented and prioritized.

6.3.4 Cyber Security R&D Planning

The Cyber Security R&D Act authorized a multi-year effort to create more secure cyber technologies, to expand cyber security R&D, and to improve the cyber security workforce. To further address cyber R&D needs, OSTP has established the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) under the NSTC. The CSIA IWG is jointly chartered by NSTC's Subcommittee on Networking and Information Technology R&D and the Subcommittee on Infrastructure. DHS co-chairs this interagency working group, which includes participation by Federal departments and agencies, as well as offices in the White House. The interagency working group coordinates policy, programs, and budgets for cyber security and information assurance R&D.

The CSIA IWG develops the Federal Plan for Cyber Security R&D, which includes near-term, mid-term, and longer term cyber security research efforts, as called for in the National Strategy to Secure Cyberspace and as directed in HSPD-7. Specific research efforts include programs to improve the security of fundamental protocols (such as Internet Protocol Version 6) and authentication technologies.

DHS identifies critical cyber R&D requirements for incorporation into this national R&D planning effort. DHS and OSTP also facilitate communications between the public and private research communities and the security community to ensure that emerging technologies are periodically reviewed by the appropriate body within the NSTC to determine possible homeland security and cyber security applications or appropriateness for inclusion in the Federal research portfolio.

6.3.5 Other R&D That Supports CI/KR Protection

Other R&D efforts that may support CI/KR protection are conducted by the SSAs and other Federal agencies. These programs address the research requirements set forth in the President's Physical and Cyber Security CI/KR Protection Strategies, which call for:

- Ensuring the compatibility of communications systems with interoperability standards;
- Exploring methods to authenticate and verify personal identity;
- Coordinating the development of CI/KR protection consensus standards; and
- Improving technical surveillance, monitoring, and detection capabilities.

For example, the Technical Support Working Group is the U.S. national forum that identifies, prioritizes, and coordinates interagency and international R&D requirements for combating terrorism. The Technical Support Working Group rapidly develops technologies and equipment to meet the high-priority needs of the combating terrorism community, including efforts that can contribute to CI/KR protection, and addresses joint international operational requirements through cooperative R&D with major allies.

Other examples of R&D that may support CI/KR protection include the SAFECOM program conducted by the DHS S&T Directorate Office of Interoperability. This program serves as the Federal umbrella to promote and coordinate initiatives between State, local, and tribal entities to develop interoperable wireless communications. SAFECOM's primary role is to work with Federal agencies and public safety personnel to define requirements and to create standards, models, and solutions to help meet those requirements.

DHS also conducts cooperative R&D programs with other Federal agencies related to authentication and verification of personal identity for the CI/KR protection workforce, and works with the American National Standards Institute and the National Institute of Standards and Technology (NIST) through the Homeland Security Standards Panel to help coordinate the development of consensus standards that support CI/KR protection.

6.3.6 Technology Pilot Programs

DHS identifies CI/KR protection needs common to certain types of assets or geographical areas while conducting site assistance, buffer zone protection visits, and other vulnerability and risk assessments. In some situations, a technological solution may be the best approach to addressing such needs. If a development program is required to create or test a potential technological solution, the DHS S&T Directorate works closely with relevant security partners to implement a technology pilot program. In some cases, this involves working with the DHS Office of Grants and Training (G&T) to identify funds and specialized training. If the pilot program is successful, the technological solutions are then implemented in other locations where similar needs exist. The following technology pilot programs illustrate some of the important capabilities that these programs can offer to security partners:

- **The National Capital Region Rail Security Corridor Pilot Project:** This project is designed to address security challenges surrounding high-risk rail infrastructure and freight traffic transiting major urban areas while maintaining fluid rail operations and meeting the needs of local law enforcement, first-responders, and the Federal Government.
- **The Constellation Automated Critical Asset Management System (Constellation/ACAMS):** This project is being developed through a partnership between DHS, the California Office of Homeland Security, and the City and County of Los Angeles. It includes a reporting capability to answer both local and national data calls on CI/KR, including information on location, size, key contacts, types of hazardous materials on site, and vulnerability assessments. It also provides for the automatic generation of BZPPs and pre-incident operational plans for local police and first-responder use in real time.
- **Coastal Surveillance Prototype Test Beds:** This iterative project is designed to provide advanced port and coastal surveillance systems. Test bed projects have been conducted in South Florida in the Port Everglades, Miami, and Key West areas, and at the Hampton Roads Sector Command Center in Virginia. Additional efforts are planned for other areas, such as Mayport, FL, and Seattle, WA.

6.4 Building, Protecting, and Maintaining Databases, Simulations, and Other Tools

Many data systems, databases, models, simulations, decision support systems, and similar information tools currently exist or are under development to enable the execution of national risk management for CI/KR.

To keep pace with the constantly evolving threat, technology, and business environments, these tools must be updated and, in some cases, new tools must be developed. Sensitive information associated with these tools must be appropriately protected. Priority efforts in this area will be focused on updating and improving key databases, developing and maintaining simulation and modeling capabilities, and coordinating with security partners on databases and modeling.

6.4.1 National CI/KR Protection Data Systems

HSPD-7 directs the Secretary of Homeland Security to implement plans and programs that identify, catalog, prioritize, and protect CI/KR in cooperation with all levels of government and private sector entities. Data systems currently provide the capability to catalog, prioritize, and protect CI/KR through such functions as:

- Maintaining an inventory of asset information and estimating the potential consequences of an attack or incident (e.g., the NADB);
- Storing information related to terrorist attacks or incidents (e.g., the National Threat and Incident Database);
- Analyzing dependencies and interdependencies (e.g., the NISAC);
- Managing the implementation of various protective programs (e.g., the BZPP Request Database); and
- Providing the continuous maintenance and updating required to enable data in these systems to reflect changes in actual circumstances.

Properly maintaining systems with current and useful data involves long-term support, coordination, and resource commitments by DHS, the SSAs, the States, private sector entities, and other security partners. Important aspects of the support, coordination, and resource commitments required over the long term to sustain the NIPP include:

- **Need for Information Protection:** Data accuracy and currency for CI/KR protection is dependent upon the ability of the various security partners to keep their databases and data systems current. Over the long term, the level of cooperation and commitment needed for this must be sustained by a trusted working relationship between various security partners. This requires that information regarded as sensitive by providers be protected from unauthorized access, use, or disclosure. Data content, accuracy, and currency must also be protected from tampering or other corruption.
- **Durable Information:** The complexity, scope, and magnitude of the U.S. CI/KR require reliance on multiple data sources that are acquired over long periods of time. As a result, information pertaining to the characteristics and quality of the data must be provided along with the actual data from each source. This requires the use of a common and standardized format, data scheme, and categorization system (i.e., taxonomy) that is viable over the long term. DHS and the SSAs are responsible for working together to establish and utilize the appropriate data collection format. The DHS taxonomy is the foundation for multiple DHS programs that focus on CI/KR information, such as the

NADB and the National Threat Incident Database. This taxonomy provides the foundation for a national-level information scheme.

- **Recurring Nature of Information Needs:** The process of information identification and additional data collection represents a recurring need. Data requirements and availability are continually reassessed based on the current threat environment, analyses to identify gaps, or other factors. Focused data calls to specific sectors or locales, in coordination with the SSAs and the States, as appropriate, may be required to fill identified information gaps. This imposes a continuing need for resources to build and update the system over the long term.

6.4.2 Simulation and Modeling

A number of security partners make use of simulations and modeling to comprehensively examine the potential consequences from terrorist attack, natural disasters, and manmade accidents that impact CI/KR, including the effects of sector and cross-sector dependencies and interdependencies. Continuous maintenance and updating are required for these tools to produce reliable projections. Over the long term, new tools are needed to address fundamental changes due to factors such as technology, threats, or the business environment.

The DHS Preparedness Directorate is the lead for modeling and simulation capabilities regarding CI/KR protection. In this capacity, the DHS Preparedness Directorate will:

- Coordinate with the DHS S&T Directorate on requirements for the development, maintenance, and application of research-related modeling capabilities for CI/KR protection;
- Specify requirements for the development, maintenance, and application of operations-related modeling capabilities for CI/KR protection in coordination with the DHS S&T Directorate and the SSAs, as appropriate;
- Coordinate with the SSAs that have relevant modeling capabilities to develop appropriate mechanisms for the development, maintenance, and use of such for CI/KR protection as directed by HSPD-7;
- Familiarize the SSAs and other security partners with the availability of relevant modeling and simulation capabilities through training and exercises;
- Work with end-users to design operations-related tools that provide maximum utility and clarity for CI/KR protection activities in both emergencies and routine operations;
- Work with end-users to design appropriate information protection plans for sensitive information used and produced by CI/KR protection modeling tools;
- Provide guidance on the vetting of modeling tools to include the use of private sector operational, technical, and business expertise where appropriate; and
- Review existing private sector modeling initiatives and opportunities for joint ventures to ensure that DHS and its security partners make maximum use of private sector modeling capabilities.

The NISAC, within DHS/OIP, provides advanced modeling and simulation capabilities for the analysis of CI/KR interdependencies, vulnerabilities, and other complex interactions. In accordance with the Homeland Security Act, DHS/OIP manages the development, maintenance, and use of relevant modeling capabilities by NISAC for CI/KR protection. NISAC technical capabilities include: data analysis; infrastructure and infrastructure interdependency modeling and simulation; decision support methodologies and tools; risk analysis; and knowledge management system design, development, and management.

NISAC activities fall into five broad categories: (1) analysis on an as-needed basis with quick turnaround time; (2) detailed analysis of infrastructure and its interdependencies; (3) risk-based decision methodology assessment, development, and implementation; (4) development of the tools and data necessary to perform and improve infrastructure analyses; and (5) support to DHS to define direction for applied R&D in support of next-generation infrastructure analysis tools.

6.4.3 Coordination With Security Partners on Databases and Modeling

Integrating existing databases into DHS databases, such as the NADB, not only reduces duplication of effort, but also ensures that available data are consistent, current, and accurate, and provide users with a consolidated picture across all CI/KR sectors. However, this approach is effective only if the source information is protected and maintained properly. Maintaining a current and useful database involves the support, coordination, and commitment of the SSAs, private

sector entities, and other security partners. Because the most current and accurate CI/KR-related data are best known by owners and operators, the effectiveness of the effort depends on all security partners keeping their databases and data systems current.

As the responsible agent for the identification of assets and existing databases for their sectors, the SSAs will:

- Outline in their SSPs the sector plans and processes for the database, data system, and modeling and simulation development and updates;
- Work with sector security partners to facilitate the collection and protection of accurate information for database, data system, and modeling and simulation use;
- Specify the timelines and milestones for the initial population of CI/KR databases; and
- Specify a regular schedule for maintenance and updating of the databases.

DHS will work with the SSAs and other security partners to:

- Identify databases and other data services that will be integrated with CI/KR protection databases and data systems;
- Facilitate the actual integration of supporting databases or importation of data into CI/KR protection databases and data systems, using a common and standardized format, data scheme, and categorization system or taxonomy specified by DHS in coordination with the SSAs; and
- Define the schedule for importing data and databases into such systems as the NADB.

6.5 Continuously Improving the NIPP and the SSPs

The NIPP uses the SCCs, GCCs, and the Government and Private Sector Cross-Sector Councils as the primary forums for coordination of policy, planning, training, and other requirements needed to ensure efficient implementation and ongoing management and maintenance of the NIPP and the SSPs.

6.5.1 Management and Coordination

DHS/OIP is the Federal executive agent for NIPP management and maintenance.

The NIPP is a multi-year plan describing mechanisms for sustaining the Nation's steady-state protective posture. The NIPP and its component SSPs include a process for annual review; periodic interim updates as required; and regularly scheduled partial reviews and re-issuance every 3 years, or more frequently, if directed by the Secretary of Homeland Security.

DHS/OIP will oversee the review and maintenance process for the NIPP; the SSAs, in coordination with the GCCs and SCCs, will establish and operate the mechanism(s) necessary to coordinate this review for their respective SSPs. The NIPP and SSP revision processes will include developing or updating any documents necessary to carry out NIPP activities. The NIPP will be reviewed at least annually to:

- Ensure that the NIPP framework is capable of measuring accomplishments in support of CI/KR protection goals and objectives and supporting the overall national approach to the homeland security mission;
- Ensure that the plan adequately reflects the organization of DHS, the SSAs, and the Federal budget process;
- Ensure that the NIPP is consistent with those Federal plans and activities that it directly supports;
- Adjust practices and procedures called for in the NIPP based on changes in the national risk management environment;
- Incorporate lessons learned and best practices from day-to-day operations, exercises, and actual incidents and alerts; and
- Reflect progress in the Nation's CI/KR protection, as well as changes to national priorities and guidance, critical tasks, sector organization, or national capabilities.

As changes are warranted, periodic updates to the NIPP will be issued. Types of developments that merit a periodic update include new laws, executive orders, Presidential directives, or regulations, and procedural changes to NIPP activities based on real-world incidents or exercise experiences.

6.5.2 Maintenance and Updating

The following paragraphs establish the procedures for posting interim changes and periodic updating of the NIPP:

- **Types of Changes:** Changes include additions of new or supplementary material and deletions. No proposed change should contradict or override authorities or other plans contained in statute, executive order, or regulation.

- **Coordination and Approval:** While DHS is the Federal executive agent for NIPP management and maintenance, any Federal department or agency with assigned responsibilities under the NIPP may propose a change to the plan. DHS is responsible for coordinating the review and approval of all proposed modifications to the NIPP with SSAs and other security partners, as appropriate. Policy changes will be coordinated and approved thorough the Homeland Security Council policy process.
- **Notice of Change:** DHS will issue an official Notice of Change for each interim revision to the NIPP. After publication, the modifications will be considered part of the NIPP for operational purposes pending a formal revision and re-issuance of the entire document. Interim changes can be further modified or updated using this process.
- **Distribution:** DHS will distribute Notices of Change to SCCs, GCCs, and other security partners. Notices of Change to other organizations will be provided upon request.
- **Re-Issuance:** DHS will coordinate full reviews and updating of the NIPP every 3 years, or more frequently, if the Secretary deems necessary. The review and updating will consider lessons learned and best practices identified during implementation in each sector and will incorporate the periodic changes and any new information technologies. DHS will distribute revised NIPP documents for interagency review and concurrence through the Homeland Security Council process.

The SSAs, in coordination with the GCCs and SCCs, will establish and operate the mechanism(s) necessary to coordinate SSP maintenance and update in accordance with the process established for the NIPP.

7. Providing Resources for the CI/KR Protection Program

Since the terrorist attacks of September 11, 2001, government and private sector expenditures to improve CI/KR protection and resilience have increased among security partners across sectors and jurisdictional levels. With finite resources available to support protection of the Nation's CI/KR, the NIPP serves as the unifying framework to ensure that CI/KR investments are coordinated and address the highest priorities, based on risk, to achieve the homeland security mission and ensure continuity of the essential infrastructure and services that support the American government, economy, and way of life.

This chapter describes an integrated, risk-based approach to fund the national CI/KR protection program and focus Federal grant assistance to State, local, and tribal entities, and complement relevant private sector activities. This integrated resource approach coordinates CI/KR protection programs and activities conducted by DHS, the SSAs, and other Federal entities through the Federal appropriations process, and focuses Federal grant funds to support national CI/KR protection efforts conducted at the State, local, and tribal levels. This resource approach also includes mechanisms to involve private sector partners in the planning process and supports collaboration among security partners to establish priorities, define requirements, share information, and maximize the use of finite resources. Implementation of this coordinated approach will help ensure that limited resources are applied efficiently and effectively to address the Nation's most critical CI/KR protection needs.

7.1 The Risk-Based Resource Allocation Process

Funding in support of CI/KR protection programs at all levels is guided by a straightforward principle: *Resources must be directed to areas of greatest priority to enable effective management of risk*. By definition, all CI/KR assets, systems, and networks are important to the Nation. However, considering the risk factors of threat, vulnerability, and consequences, some assets, systems, networks, or functions are deemed to be more critical to the Nation, as a whole, than others. This chapter provides a process to ensure that the Nation's CI/KR protection resource requirements are correctly identified and appropriately prioritized to meet the Nation's most critical protection needs. Using a risk-based approach, DHS collaborates with other security partners to identify those assets, systems, networks, and functions that are most critical from a national perspective, and lead, integrate, and coordinate a cohesive effort to help ensure their protection. Through the NIPP framework, DHS works with the SSAs, States, and other government and private sector security partners to gain an understanding of how CI/KR protection is being conducted across the country, what priorities and requirements drive these efforts, and how such efforts are funded. This assessment helps DHS to identify duplicative efforts and gaps in CI/KR protection across sectors and jurisdictions. DHS then uses the information gained to recommend funding targeted at the appropriate CI/KR protec-

tive programs or activities that help ensure that government resources are allocated to the areas of greatest priority.

7.1.1 Sector-Specific Agency Reporting to DHS

Given their unique capabilities and individual risk landscapes, CI/KR sectors each face different protection challenges. For instance, some sectors have distinct, easily identifiable assets that can be logically prioritized. Some have thousands of identical assets, not all of which are equally critical. Others are made up of systems or networks, as opposed to distinct assets, for which the identification of specific protective measures may prove to be impossibly complex. Furthermore, interdependencies among sectors can cause duplicative protection efforts or lead to gaps in funding for CI/KR protection. To ensure that resources are allocated according to national priorities and are based on national risk and need, DHS must be able to accurately assess priorities, requirements, and efforts across these diverse sectors.

As DHS conducts this assessment, the SSAs, supported by their respective SCCs and GCCs, provide information regarding their sectors' individual CI/KR protection efforts. The SCCs participate in the process to ensure that private sector input is reflected in SSA reporting of sector priorities and requirements. The first step for an SSA in the risk-based resource allocation process is to coordinate with sector partners, including SCCs and GCCs as appropriate, to accurately determine sector priorities, program requirements, and funding needs for CI/KR protection. HSPD-7 requires each SSA to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors. Consistent with this requirement, DHS will provide the SSAs with reporting guidance and templates that include requests for specific information, such as CI/KR protection priorities, requirements, and resources. The following elements should be included in the Sector CI/KR Protection Annual Report to help inform prioritization resource allocation recommendations:

- Priorities and annual goals for CI/KR protection and associated gaps;
- Sector-specific requirements for CI/KR protection activities and programs based on risk and need; and
- Projected CI/KR-related resource requirements for the sector, with an emphasis on anticipated gaps or shortfalls in funding for sector-level CI/KR protection and/or for protection efforts related to national-level CI/KR that exist within the sector.

7.1.2 State Government Reporting to DHS

Like sectors, State governments face diverse CI/KR protection challenges and have different priorities, requirements, and available resources. Furthermore, State CI/KR protection efforts are closely intertwined with those of other government and private sector partners. In particular, States work closely with local and tribal governments to address CI/KR protection challenges at those levels. To accurately assess the national CI/KR protection effort and identify protection needs that warrant attention at a national level, DHS must aggregate information across State jurisdictions as it does across sectors.

DHS requires that each State develop a homeland security strategy that establishes goals and objectives for its homeland security program that include CI/KR protection as a core element. State administrative agencies develop a Program and Capability Enhancement Plan that prioritizes statewide resource needs to support this program. The State administrative agency works with DHS to identify:

- Priorities and annual goals for CI/KR protection;
- State-specific requirements for CI/KR protection activities and programs, based on risk and need;
- Mechanisms for coordinated planning and information sharing with government and private sector security partners;
- Unfunded CI/KR protection initiatives or requirements that should be considered for funding using Federal grants (described in further detail below); and
- Other funding sources utilized to implement the NIPP and address identified priorities and annual goals.

For consideration in the deliberations related to CI/KR protection resources as part of the Federal budget cycle, information on statewide CI/KR resources needs must be reported to DHS by the date specified in the appropriate annual DHS/G&T planning guidance. DHS/G&T will include information such as model reports or report templates with the planning guidance to support the States' reporting efforts.

7.1.3 Aggregating Submissions to DHS

DHS will use the information collected from the SSA Sector CI/KR Protection Annual Reports and State reports to DHS/G&T to assess CI/KR protection status and requirements across the country. As national priorities and requirements are established, DHS will develop funding recom-

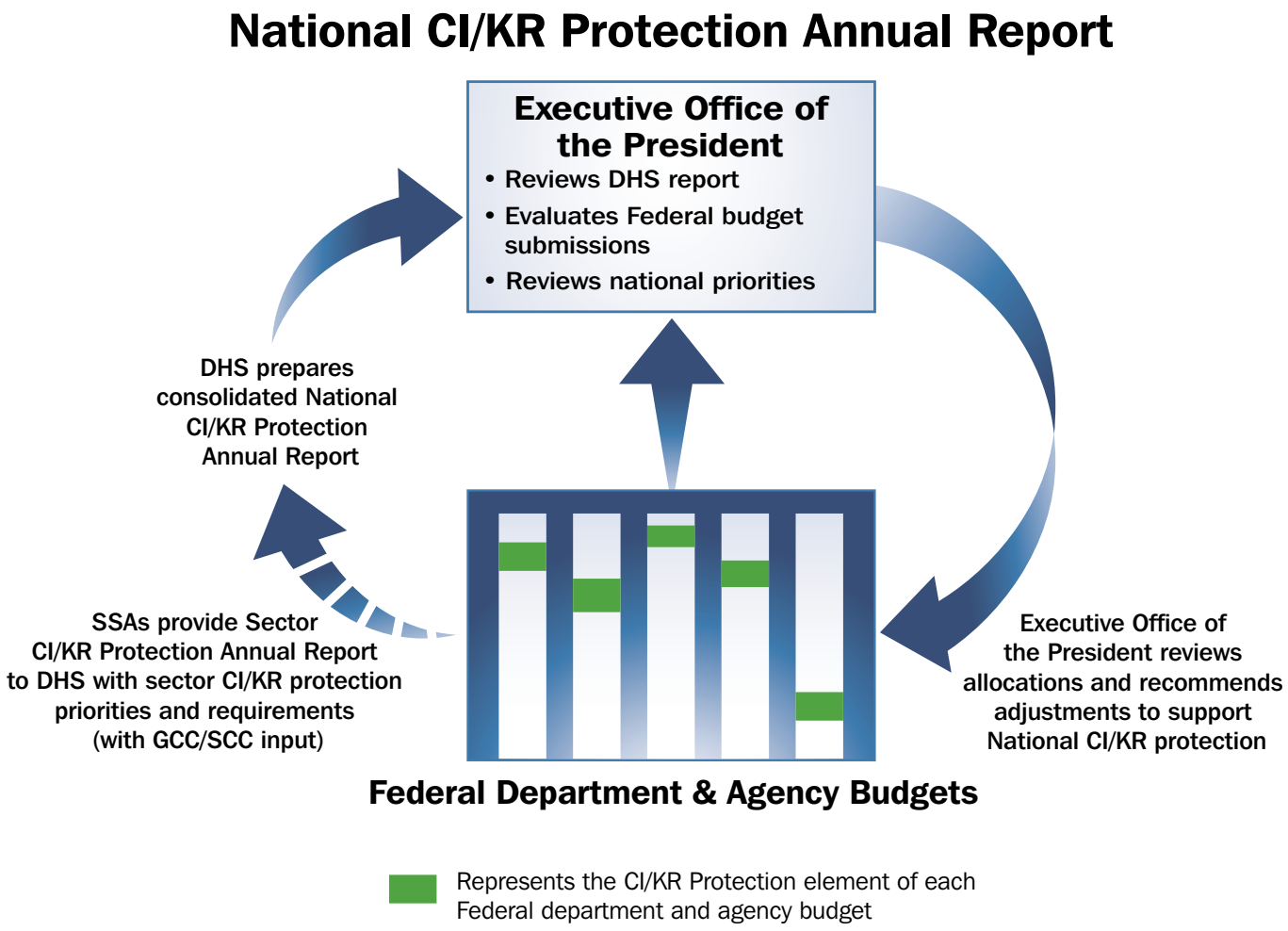
mendations for programs and initiatives designed to reduce national-level risk in the CI/KR protection mission area. In cases where gaps or duplicative efforts exist, DHS will work with the SSAs and the States to identify strategies or additional funding sources to help ensure that national CI/KR protection priorities are efficiently and effectively addressed.

Following the collection and aggregation of sector- and State-level reports, DHS will summarize this information in the National CI/KR Protection Annual Report. This report will provide a summary of national CI/KR protection priorities and requirements and make recommendations for prioritized resource allocation across the Federal Government to meet national-level CI/KR protection needs. The National CI/KR Protection Annual Report will be submitted along with the DHS budget submission to the Executive Office of the President on or before September 1 as part of the annual Federal budget process (see figure 7-1).

7.2 Federal Resource Allocation Process for DHS, the SSAs, and Other Federal Agencies

The Federal resource allocation process described in this section is designed to ensure that the collective efforts of DHS, the SSAs, and other Federal departments and agencies support the NIPP and national priorities. It is also designed to be consistent with the DHS responsibility to coordinate overall national CI/KR protection and to identify national-level gaps, overlaps, or shortfalls. Driven in large part by existing and well-understood Federal budget process milestones, this approach will be integrated with the established Federal budget process and reporting requirements. The resource allocation process for CI/KR protection outlined in this chapter recognizes the existing budget authorities and responsibilities of all Federal departments and agencies with CI/KR protection-related programs and activities. The NIPP process

Figure 7-1: National CI/KR Protection Annual Report Process



aims to create synergy between current and future efforts to ensure a unified and effective national CI/KR protection effort. The specific roles of DHS and the SSAs are described in further detail below.

7.2.1 Department of Homeland Security

DHS is responsible for overall coordination of the Nation's CI/KR protection efforts. To carry out this responsibility, DHS must identify and prioritize nationally critical assets, systems, and networks; help ensure that appropriate protective initiatives are implemented; and help address any gaps or shortfalls in the protection of nationally critical CI/KR. DHS works closely with the Executive Office of the President to aggregate CI/KR protection-related activities and related resource requests from the SSAs and other Federal departments and agencies as a way to make informed tradeoffs in prioritizing Federal investments.

DHS will work with the Executive Office of the President offices to establish a national CI/KR protection strategic approach and priorities, and with the SSAs, supported by their respective SCCs and GCCs, to develop sector-specific CI/KR protection-related requirements. Driven largely by the identification and prioritization of critical assets, systems, networks, and functions across sectors and States, the establishment of national protection priorities will help inform resource allocation decisions later in the process. SSAs communicate information about their existing CI/KR protection-related programs and outstanding requirements to DHS through their Sector CI/KR Protection Annual Reports. DHS uses the sector annual reports to inform the National CI/KR Protection Annual Report. The National CI/KR

Figure 7-2: National CI/KR Protection Annual Report Analysis

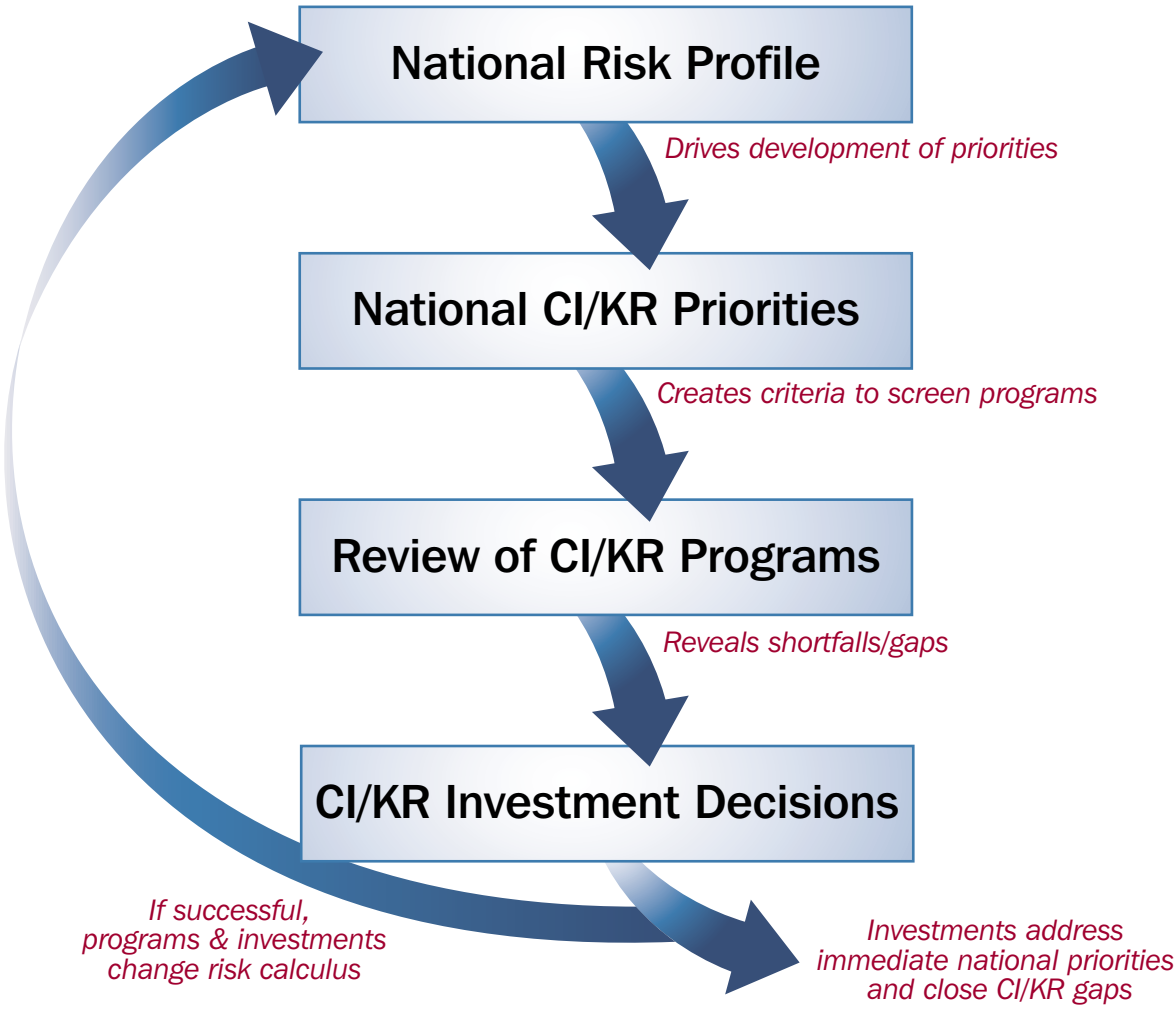


Figure 7-3: DHS and SSA Roles and Responsibilities in Federal Resource Allocation

	DHS	Sector-Specific Agencies
Feb-July	• Work with HSC to establish national NIPP priorities • Through partnership mechanisms such as SCCs and GCCs, work with SSAs to develop national and sector-specific **NIPP requirements**	• Work with DHS in development of national and sector-specific NIPP requirements • Develop NIPP-related aspect of budget submission with support of DHS where necessary and consistent with NIPP requirements established through collaborative process
July-Sep	• Aggregate **Annual Reports** from all sectors to develop picture of national NIPP-related priorities and requirements • Submit **National CI/KR Protection Annual Report** on **September 1**	• On **July 1**, submit Sector CI/KR Protection Annual Report to DHS that includes summary of existing **NIPP-related programs**
Sep-Nov	• Work with OMB and SSAs to remedy any gaps or shortcomings in NIPP-related funding, focusing on ensuring funding of programs associated with **nationally critical assets, systems, networks, or functions**	• Work with OMB and DHS in subsequent budget deliberations to remedy any **gaps or shortfalls** in NIPP-related funding

Protection Annual Report analyzes information about sector priorities, requirements, and programs in the context of the National Risk Profile, a high-level summary of the aggregate risk and protective status of all sectors. The National Risk Profile drives the development of national priorities, which, in turn, are used to assess existing CI/KR programs and to identify existing gaps or shortfalls in national CI/KR protection efforts. This analysis provides the Executive Office of the President with information that supports both strategic and investment decisions related to CI/KR protection.

7.2.2 Sector-Specific Agencies

Earlier chapters of the NIPP articulate how DHS and the SSAs will work with the respective CI/KR sectors to determine risk and set priorities. Based on guidance from DHS, each SSA will develop and maintain an SSP that supports the NIPP goal and supporting objectives. Additionally, the SSAs, in partnership with the SCCs and GCCs, are asked to determine sector-specific priorities and requirements for CI/KR protection. The SSAs submit these priorities and requirements to DHS in their sector annual reports, along with identification of resource needs, to allow for a more comprehensive National CI/KR Protection Annual Report. SSAs will work within their respective department or agency budget process to determine the CI/KR protection-related aspects of their department's budget submission. SSA annual reports are submitted to DHS on or before July 1 of each year. Resource information contained in the SSA annual reports is based on appropriated funding, as well as the President's most recent budget.

Additionally, the subset of CI/KR protection funding requirements directed toward R&D and S&T investments will be highlighted by the SSAs, SCCs, and GCCs in the sector annual

reports to inform the NCIP R&D Plan and its technology roadmap, while ensuring efficient coordination with the DHS R&D/S&T community and supporting the Federal research and technology base. These R&D and S&T plans and requirements will be based on the R&D planning section of each sector's SSP. The identified R&D requirements will be prioritized based on the potential increase in CI/KR protection capabilities for a given investment.

7.2.3 Summary of Roles and Responsibilities

Figure 7-2 outlines the roles and responsibilities of DHS and the SSAs throughout this process, as well as the annual timelines associated with major activities.

The final determination of funding priorities, based on the collaborative efforts of DHS, the SSAs and other Federal departments and agencies, and the Executive Office of the President, will guide CI/KR protection programs and the allocation of resources in support of the NIPP. These priorities will support Federal Government (DHS and SSA) CI/KR protection activities, as well as guide and support homeland security and CI/KR protection activities across and within State, local, and tribal jurisdictions.

7.3 Federal Resources for State and Local Government Preparedness

Federal grants from DHS and Federal agencies, and other programs, such as training and technical assistance, offer key support to State and local jurisdictions for CI/KR protection programs. These grants and other programs provide resources to meet CI/KR needs that are managed by State and local entities.

DHS/G&T is responsible for coordinating Federal homeland security grant programs to help State, local, and tribal governments enhance their ability to prevent, protect against, respond to, and recover from terrorist acts or threats and other hazards. DHS/G&T offers State, local, and tribal security partners access to funding through several grant programs that can be leveraged to support CI/KR protection requirements based on risk and need.

For the purposes of the NIPP, Federal grants available through DHS/G&T can be grouped into two broad categories: (1) overarching homeland security programs that provide funding for a broad set of activities in support of homeland security mission areas and the national priorities outlined in the National Preparedness Goal, and (2) targeted infrastructure protection programs for specific CI/KR-related protection initiatives and programs within identified jurisdictions. States should leverage the range of available resources, including those from Federal, State, local, and tribal sources, as appropriate, in support of the protection activities needed to reduce vulnerabilities and close identified capability gaps related to CI/KR within their jurisdictions.

Overarching Homeland Security Programs: The Overarching Homeland Security Grant Program supports activities that are conducted in accordance with the National Preparedness Goal. These funds support overall State and local homeland security efforts, and can be leveraged to support State, regional, local, and/or tribal CI/KR protection. These funds are intended to complement and be allocated in coordination with national CI/KR protection efforts.

The primary overarching homeland security grant programs include:

- **State Homeland Security Program:** The SHSP supports the implementation of the State Homeland Security Strategy to address identified planning, equipment, training, and exercise needs for acts of terrorism. In addition, SHSP supports the implementation of the National Preparedness Goal, the NIMS, the NRP, and the NIPP to support the prevention of, protection against, response to, and recovery from acts of terrorism.
- **Urban Areas Security Initiative:** UASI funds address the unique planning, equipment, training, and exercise needs of high-threat, high-density urban areas, and assist them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism.

Targeted Infrastructure Protection Programs: Targeted infrastructure protection programs include grants for specific activities that focus on the protection of CI/KR, such as ports, mass transit, rail transportation, etc. These funds support CI/KR protection capabilities based on risk and need in coordination with DHS, SSAs, and Federal agencies. Though recent appropriations have been divided among specific sectors, DHS seeks to combine these grants into a program that supports a more integrated risk-based approach across CI/KR sectors.

DHS/OIP and DHS/G&T will work with States to focus targeted infrastructure protection grant programs, such as the BZPP and transportation security grants, to support national-level CI/KR protection priorities and to reinforce activities funded through Federal department and agency budgets and other homeland security grant programs. As appropriate,

SSAs serve as subject matter experts reviewing and providing recommendations for specific target grant programs. Grantees should apply resources available under the overarching homeland security grant programs, such as SHSP and UASI to address their regionally or locally critical priority CI/KR protection initiatives. A further prioritized combination of grant funding across various programs may be necessary to enable the protection of certain assets, systems, networks, and functions deemed to be nationally critical.

Available DHS/G&T grant funding is awarded to the Governor-appointed State administrative agency, which serves in each State as the lead for program implementation. Through the State administrative agencies, States will identify and prioritize their homeland security needs, including CI/KR protection, and leverage assistance from these funding streams to accomplish the priorities identified in their State Homeland Security Strategies, and Program and Capability Enhancement Plans. These planning processes undertaken at the State level are built on the common framework articulated in the National Preparedness Goal; the National Priorities, including implementation of the NIPP; and capabilities enhancements based on the TCL.

DHS will provide State, local, and tribal authorities with additional guidance on how to identify, assess, and prioritize CI/KR protection needs and programs in support of the National Preparedness Goal as they apply for homeland security grants. Additional information on DHS grant programs, guidelines, allocations, and eligibility is available at: www.ojp.usdoj.gov/odp/.

7.4 Other Federal Grant Programs That Contribute to CI/KR Protection

Other Federal departments and agencies provide grant programs that can contribute to CI/KR protection. These are usually sector- or threat-specific programs; many are related to technology development initiatives. Examples of these grant programs include:

- **Department of Energy:** DOE manages grant programs for the development of technologies for assurance of the U.S. energy infrastructure. These programs address the development and demonstration of technologies and methodologies to protect physical energy infrastructure assets. Technologies and methodologies of relevance are those that accomplish security and reliability functions such as hardening of assets; surveillance; non-invasive inspection of sealed containers; remote detection; and characterization of damage, entry control, perimeter monitoring, detection of explosives, and improved electricity reliability.
- **Department of the Interior:** The Bureau of Indian Affairs manages a grant program for the Safety of Dams on Indian Lands with the objective of improving the structural integrity of dams on Indian lands. Financial awards are specific to a given site; awards are restricted to Indian tribes or tribal organizations.
- **Department of Justice:** The National Institute of Justice (NIJ), Office of Justice Programs, manages a grant program for Domestic Anti-Terrorism Technology Development. The objective of the program is to support the development of counterterrorism technologies, assist in the development of standards for those technologies, and work with State and local jurisdictions to identify particular areas of vulnerability to terrorist acts and to be better prepared to respond if such acts occur. The NIJ is authorized to make grants to, or enter into contracts or cooperative agreements with, State and local governments, private nonprofit organizations, public nonprofit organizations, for profit organizations, institutions of higher education, and qualified individuals. Applicants from the Territories of the United States and federally recognized Indian tribal governments are also eligible to participate in this program.
- **Department of Transportation:** The Pipeline and Hazardous Materials Safety Administration Pipeline Safety grant program supports efforts to develop and maintain State natural gas, liquefied natural gas, and hazardous liquid pipeline safety programs. Grant recipients are typically State government agencies.
- **Department of Transportation:** The Federal Transit Administration is a grants-in-aid agency that has several major assistance programs for eligible activities. Funds are provided through legislative formulas or discretionary authority. Funding from these programs is provided on an 80/20 Federal/local funding match basis, unless otherwise specified. These assistance programs can contribute to CI/KR protection efforts through funding for metropolitan and State planning and research grants; urban, non-urban, and rural transit assistance programs; bus and railway modernization efforts; major capital investments; and special flexible-funding programs.

These programs are available to a wide range of grant recipients, including CI/KR owners and operators and State, local, and tribal governments.

7.5 Setting an Agenda in Collaboration With CI/KR Protection Security Partners

Resource allocation decisions for CI/KR protection at all levels of government should align as integral components of the unified national approach established in the NIPP. In accordance with the responsibilities established in HSPD-7, DHS works with the SSAs and other government and private sector security partners to set the national agenda that specifies this strategic approach to CI/KR protection, articulates associated requirements, supports collaboration among security partners, and recognizes the contributions of private sector partners to the overall effort. While Federal Government funding of programs and initiatives that support CI/KR protection makes a significant contribution to the security of the Nation, a fully successful effort requires DHS; the SSAs; and State, local, and tribal governments to work closely with the private sector to promote the most effective use of Federal and non-Federal resources.

The NIPP uses the risk management framework to support coordination between security partners outside the Federal Government. Each step of the risk management framework presents opportunities for collaboration between and among all security partners. Coordination between State and local agencies and the sectors themselves ensures that cross-sector needs and priorities are more accurately identified and understood. Government coordination with private sector owners and operators at all levels is required throughout the process to ensure a unified national CI/KR protection effort; provide accurate, secure identification of CI/KR assets and systems; provide and protect risk-related information; ensure implementation of appropriate protective measures; measure program effectiveness; and make required improvements.

These opportunities for collaboration allow private sector owners and operators to benefit from CI/KR protection investments in a number of ways. First, investments in CI/KR protection will enable risk mitigation in a broader, all-hazards context, including common threats posed by malicious individuals or acts of nature, in addition to those posed by terrorist organizations. Second, continuity-of-business planning can facilitate recovery of commercial activity after an incident. Finally, investing in CI/KR protection within the NIPP framework will help private sector owners and operators enhance protective measures, and will support decisionmaking with more comprehensive risk-based information. DHS explores new opportunities to encourage such collaboration through incentives (such as the SAFETY Act), which creates liability protection for sellers of qualified anti-terrorism technologies), regulatory changes, and by providing more useful information on risk assessment and management. While States typically are the eligible applicants for DHS grant programs, certain private sector entities can apply directly for grant funds through programs such as the Port Security Grant Program and the Intercity Bus Security Grant Program.

More information about the NIPP is available on the Internet at:
www.dhs.gov/nipp or by contacting DHS at:
nipp@dhs.gov

Example: Leveraging Resources to Support Homeland Security and CI/KR Protection Activities of a Mass Transit System

The following example provides an illustration of how the various funding sources described in this chapter can work together in a practical situation to address the CI/KR protection needs of a local system that, through implementation of the NIPP risk management framework and SSP processes, is deemed to be critical to the Nation. This example focuses on a mass transit system in a community that participates in the UASI program.

In this situation, the following resources may be applied to support the safety and security of the mass transit system:

Owner/Operator Responsibilities

The local mass transit authority, as the owner and operator of the system, funds system-specific protection and security measures, including resiliency and business continuity planning activities, for the system on a day-to-day basis.

State, Local, and Tribal Government Responsibilities

State, local, and tribal governments support the day-to-day protection of the public; enforce security, protective, and preventive measures around the system's facilities; and provide response and/or recovery capabilities should an incident occur.

Federal Support and Grant Funding

Assistance from the Federal Government through a variety of resources, including grants (both targeted infrastructure protection grant programs and overarching homeland security grant programs), training, technical assistance, and exercises, further support and enhance ongoing homeland security and CI/KR protection activities. In this example, DHS, as the SSA for the Transportation sector; TSA; DOT; and the USCG may contribute to the protection efforts through either appropriated program funds or grants. Based on eligibility, a range of grants may support the overall protection of this system, including:

- If the mass transit system is eligible for targeted infrastructure protection program funding, such as the Transit Security Grant Program, this funding source may be leveraged to support security enhancements for the mass transit system.
- If the mass transit system is eligible under the BZPP, this funding source may also be leveraged to improve security around the system or enhance preparedness capabilities within the surrounding community.
- Homeland Security grant program funding from programs such as the SHSP, UASI, and Law Enforcement Terrorism Prevention Program may be leveraged to enhance prevention, protection, response, and recovery capabilities in and around the mass transit system if the system is deemed critical by the State and/or local authorities within their homeland security strategies and priorities, and in accordance with allowable cost guidance.
- The Assistance to Firefighters Grant Program may be leveraged to support preparedness capabilities of the local fire department that are necessary to protect the system within the city.
- Federal Transit Administration grant programs to support metropolitan and State planning may be leveraged to provide planning for upgrades to the system, which include more resilient CI/KR design, and the major capital investments and special flexible-funding grant programs may be leveraged to help build these improvements.

All of these resources, used in support of the region's mass transit system, are coordinated with State and urban area homeland security strategies, as well as the applicable Regional Transit Security Strategy. Additionally, other services, training, exercises, and/or technical assistance (for example, the DHS/G&T Mass Transit Technical Assistance Program, which includes a facilitated risk assessment) may be leveraged from a variety of Federal partners.

List of Acronyms and Abbreviations

ACAMS	Automated Critical Asset Management System
BZPP	Buffer Zone Protection Program
CAEIAE	Centers of Academic Excellence in Information Assurance Education
CEO	Chief Executive Officer
CFIUS	Committee on Foreign Investment in the United States
CFR	Code of Federal Regulations
CII	Critical Infrastructure Information
CI/KR	Critical Infrastructure and Key Resources
CIPAC	Critical Infrastructure Partnership Advisory Council
COI	Community of Interest
CSIA IWG	Cyber Security and Information Assurance Interagency Working Group
CSIRT	Computer Security Incident Response Teams
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
ECTF	Electronic Crimes Task Force
E.O.	Executive Order
EOP	Executive Office of the President
FACA	Federal Advisory Committee Act
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIRST	Forum of Incident Response and Security Teams
FOIA	Freedom of Information Act
FSLC	Federal Senior Leadership Council
G&T	Grants and Training Office (Division of DHS Preparedness Directorate)
GCC	Government Coordinating Council
GFIRST	Government Forum of Incident Response and Security Teams
GPS	Global Positioning System
GSA	General Services Administration
HHS	Department of Health and Human Services
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HMGP	Hazard Mitigation Grant Program
HSAC	Homeland Security Advisory Council
HSAS	Homeland Security Advisory System
HSEEP	Homeland Security Exercise and Evaluation Program
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network for Critical Sectors
HSPD	Homeland Security Presidential Directive
iCAV	Infrastructure and Critical Asset Viewer
ISAC	Information Sharing and Analysis Center
ISE	Information-Sharing Environment
IWWN	International Watch and Warning Network
JCG	Joint Contact Group
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Online
MIFC	Maritime Intelligence Fusion Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NADB	National Asset Database
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center for Telecommunications

NCIP R&D	National Critical Infrastructure Protection Research and Development
NCRCG	National Cyber Response Coordination Group
NCS	National Communications System
NCSA	National Cyber Security Alliance
NCTC	National Counterterrorism Center
NHC	National Hurricane Center
NIAC	National Infrastructure Advisory Council
NIAP	National Information Assurance Partnership
NICC	National Infrastructure Coordinating Center
NIJ	National Institute of Justice
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NIST	National Institute of Standards and Technology
NJTTF	National Joint Terrorism Task Force
NOC	National Operations Center
NOC-HQE	National Operations Center – Headquarters Element
NRC	Nuclear Regulatory Commission
NRCC	National Response Coordination Center
NRP	National Response Plan
NSA	National Security Agency
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
OAS	Organization of American States
OCA	Original Classification Authority
OECD	Organisation for Economic Co-operation and Development
OI&A	Office of Intelligence and Analysis (Division of DHS Preparedness Directorate
OIP	Office of Infrastructure Protection (Division of DHS Preparedness Directorate)
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PCC	Policy Coordinating Committee
PCII	Protected Critical Infrastructure Information
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
PSA	Protective Security Advisor
PVTSAC	Private Sector Senior Advisory Committee
RAMCAP	Risk Analysis and Management for Critical Asset Protection
R&D	Research and Development
RISS	Regional Information Sharing Systems
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SHSP	State Homeland Security Program
SLTGCC	State, Local, and Tribal Government Coordinating Council
SPP	Security and Prosperity Partnership of North America
SSA	Sector-Specific Agency
SSI	Sensitive Security Information
SSP	Sector-Specific Plan
S&T	Science and Technology Directorate of DHS
SVA	Security Vulnerability Assessment
TCL	Target Capabilities List
TSA	Transportation Security Administration
UASI	Urban Areas Security Initiative
UCNI	Unclassified Controlled Nuclear Information
U.S.	United States
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
UTL	Universal Task List
WMD	Weapons of Mass Destruction

Glossary of Key Terms

Many of the definitions in this Glossary are derived from language enacted in Federal laws and/or included in national plans, including the Homeland Security Act of 2002, USA PATRIOT Act of 2001, the National Incident Management System, and the National Response Plan.

All-Hazards. An approach for prevention, protection, preparedness, response, and recovery that addresses a full range of threats and hazards, including domestic terrorist attacks, natural and manmade disasters, accidental disruptions, and other emergencies.

Asset. Contracts, facilities, property, electronic and non-electronic records and documents, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

Business Continuity. The ability of an organization to continue to function before, during, and after a disaster.

Consequence. The result of a terrorist attack or other hazard that reflects the level, duration, and nature of the loss resulting from the incident. For the purposes of the NIPP, consequences are divided into four main categories: public health and safety, economic, psychological, and governance impacts.

Control Systems. Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include SCADA systems, Process Control Systems, and Digital Control Systems.

Critical Infrastructure. Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.

Critical Infrastructure Information. Information not customarily in the public domain related to the security of critical infrastructure or protected systems, and voluntarily provided to the government. CII includes any planned or past assessment, projection, estimate, operational problem, or solution regarding critical infrastructure or protected systems' ability to resist any actual, potential, or threatened unlawful interference with, attack on, compromise of, or incapacitation of this infrastructure or systems by either physical or computer-based attack.

Cyber Security. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

Dependency. The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Function. In the context of the NIPP, function is defined as the service, process, capability, or operation performed by specific infrastructure assets, systems, or networks.

Government Coordinating Council. The government counterpart to the SCC for each sector established to enable interagency coordination. The GCC is comprised of representatives across various levels of government (Federal, State, Territorial, local, and tribal) as appropriate to the security and operational landscape of each individual sector.

Hazard. Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

Incident. An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements.

Interdependency. The multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Key Resources. As defined in the Homeland Security Act, "key resources" are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Mitigation. Activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident. Mitigation measures are often developed in accordance with lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Measures may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury.

Network. In the context of the NIPP, a group of assets or systems that share information or interact with each other in order to provide infrastructure services within or across sectors.

Normalize. In the context of the NIPP, the process of transforming risk-related data into comparable units.

Owners/Operators. Those entities responsible for day-to-day operation and investment in a particular asset or system.

Preparedness. The range of deliberate critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required activities and resources to mitigate risk.

Prevention. Actions taken to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property. Involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; immunizations, isolation, or quarantine; public health and agricultural surveillance and testing processes; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Prioritization. In the context of the NIPP, prioritization is the process of using risk assessment results to identify where risk-reduction or mitigation efforts are most needed and subsequently determine which protective actions should be instituted in order to have the greatest effect.

Protection. Actions to mitigate the overall risk to CI/KR assets, systems, networks, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, protection includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, and implementing cyber security measures, among various others.

Recovery. The development, coordination, and execution of service- and site-restoration plans for impacted communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents.

Resiliency. In the context of the NIPP, resiliency is the capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident.

Response. Activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs.

Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk. A measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the NIPP, risk is the expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss.

Risk Management Framework. A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risks; prioritizing and implementing protective programs; measuring performance; and taking corrective action. Public and private sector entities often include risk management frameworks in their business continuity plans.

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The NIPP addresses 17 CI/KR sectors as defined in HSPD-7.

Sector Coordinating Council. The private sector counterpart to the GCCs, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of CI/KR protection activities and issues.

Sector Partnership Model. The framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CI/KR protection involving all levels of government and private sector entities.

Sector-Specific Agency. Federal departments and agencies identified in HSPD-7 as responsible for CI/KR protection activities in specified CI/KR sectors.

Sector-Specific Plan. Augmenting plans that complement and extend the NIPP Base Plan and detail the application of the NIPP framework specific to each CI/KR sector. SSPs are developed by the SSAs in close collaboration with other security partners.

Security Partner. Those Federal, State, regional, Territorial, local, or tribal government entities, private sector owners and operators and representative organizations, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's CI/KR.

Steady-State. In the context of the NIPP, steady-state is the posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents.

System. In the context of the NIPP, a system is a collection of assets, resources, or elements that performs a process that provides infrastructure services to the Nation.

Terrorism. Any activity that: (1) involves an act that is (a) dangerous to human life or potentially destructive of critical infrastructure or key resources, and (b) a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (2) appears to be intended to (a) intimidate or coerce a civilian population, (b) influence the policy of a government by intimidation or coercion, or (c) affect the conduct of a government by mass destruction, assassination, or kidnapping.

Threat. The intention and capability of an adversary to undertake actions that would be detrimental to CI/KR.

Value Proposition. A statement that outlines the national and homeland security interest in protecting the Nation's CI/KR and articulates benefits gained by all security partners through the risk management framework and public-private partnership described in the NIPP.

Vulnerability. A weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or disrupted by a natural hazard or technological failure.

Weapons of Mass Destruction. (1) Any explosive, incendiary, or poison gas (i) bomb, (ii) grenade, (iii) rocket having a propellant charge of more than 4 ounces, (iv) missile having an explosive or incendiary charge of more than one-quarter ounce, or (v) mine or (vi) similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (18 U.S.C. 2332a).

Appendix 1: Special Considerations

Appendix 1A: Cross-Sector Cyber Security

This appendix provides additional details on the processes, procedures, and mechanisms needed to achieve NIPP goals and supporting objectives regarding cyber security. It specifies cyber security roles and responsibilities, coordination processes, initiatives to mitigate risk, and milestones and metrics to measure progress.

This appendix provides information concerning the *users* of cyber infrastructure, including the various CI/KR sectors and their associated security partners. Matters concerning *producers and providers* of cyber infrastructure (i.e., the Information Technology and Telecommunications sectors) are addressed in the SSPs. This appendix is organized to align with the corresponding chapters of the NIPP to provide the reader with the context for the additional information as follows:

1A.1 Introduction

The U.S. economy and national security are highly dependent upon cyber infrastructure. Cyber infrastructure enables the Nation's essential services, resulting in a highly interconnected and interdependent network of CI/KR. This network provides services supporting business processes and financial markets, and also assists in the control of many critical processes, including the electric power grid and chemical processing plants, among various others.

A spectrum of malicious actors can and do conduct attacks against critical cyber infrastructure on an ongoing basis. Of primary concern is the risk of organized cyber attacks capable of causing debilitating disruption to the Nation's CI/KR,

economy, or national security. Furthermore, while terrorist groups have not yet initiated a major attack against the Internet, there is evidence of their using it as a more limited means of attack or for other purposes that support terrorist activities.

DHS and the SSAs are committed to working collaboratively with other public, private, academic, and international entities to enhance cyber security awareness and preparedness efforts, and ensure that the cyber elements of CI/KR are:

- Robust enough to withstand attacks without incurring catastrophic damage;
- Responsive enough to recover from attacks in a timely manner; and
- Resilient enough to sustain nationally critical operations.

1A.1.1 Value Proposition for Cyber Security

The value proposition for cyber security aligns with that for CI/KR protection in general, as discussed in chapter 1 of the NIPP Base Plan, but with a concentrated focus on cyber infrastructure. Many CI/KR functions and services are enabled through cyber systems and services; if cyber security is not appropriately addressed, the risk to CI/KR is increased. The responsibility for cyber security spans all security partners, including public and private sector entities and individual citizens. The NIPP provides a coordinated and collaborative approach to help public and private sector security partners and individual citizens understand and manage cyber risk.

The NIPP promotes cyber security by facilitating participation and partnership in CI/KR protection initiatives, leveraging cyber-specific expertise and experience, and improving information exchange and awareness of cyber security concerns. It also provides a framework for public and private sector security partner efforts to recognize and address similarities and differences between approaches to cyber risk management for business continuity and national security. This framework enables security partners to work collaboratively to make informed cyber risk management decisions, define national cyber priorities, and address cyber security as part of an overall national CI/KR protection strategy.

1A.1.2 Definitions

The following definitions explain key terms and concepts related to the cyber dimension of CI/KR protection:

- **Cyber infrastructure:** Includes electronic information and communications systems and services and the information contained therein. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications includes sharing and distribution of information. For example, computer systems; control systems (e.g., SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure:
  - *Producers and providers* of cyber infrastructure represent the information technology industrial base, and comprise the Information Technology sector. The producers and providers of cyber infrastructure play a key role in developing secure and reliable products and services.
  - *Consumers* of cyber infrastructure must maintain its security as new vulnerabilities are identified and the threat environment evolves. Individuals, whether private citizens or employees with cyber systems administration responsibility, play a significant role in managing the security of computer systems to ensure that they are not used to enable attacks against CI/KR.
- **Cyber Security:** The prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and services (and the information contained therein) to ensure confidentiality, integrity, and availability.

- **Cross-Sector Cyber Security:** Collaborative efforts between DHS, the SSAs, and other security partners to improve the cyber security of the CI/KR sectors by facilitating cyber risk-mitigation activities.

1A.1.3 Cyber-Specific Authorities

Various Federal strategies, directives, policies, and regulations provide the basis for Federal actions and activities associated with implementing the cyber-specific aspects of the NIPP. The three primary authorities associated with cyber security are the National Strategy to Secure Cyberspace, HSPD-7, and the Homeland Security Act. These documents are described in further detail in appendix 2A of the NIPP.

1A.2 Cyber Security Responsibilities

The National Strategy to Secure Cyberspace, HSPD-7, and the Homeland Security Act identify the responsibilities of the various security partners with a role in securing cyberspace. These roles and responsibilities are described in more detail below.

1A.2.1 Department of Homeland Security

In accordance with HSPD-7, DHS is a principal focal point for the security of cyberspace. DHS has specific responsibilities regarding the coordination of the efforts of security partners to prevent damage to, unauthorized use and exploitation of, and enable the restoration of cyber infrastructure to ensure confidentiality, integrity, and availability. These responsibilities include:

- Developing a comprehensive national plan for securing U.S. CI/KR;
- Providing crisis management in response to incidents involving cyber infrastructure;
- Providing technical assistance to other government entities and the private sector with respect to emergency recovery plans for incidents involving cyber infrastructure;
- Coordinating with other Federal agencies to provide specific warning information and advice on appropriate protective measures and countermeasures to State, local, and tribal governments; the private sector; academia; and the public;
- Conducting and funding cyber security R&D, in partnership with other agencies, which will lead to new scientific understanding and technologies in support of homeland security; and
- Assisting SSAs in understanding and mitigating cyber risk and in developing effective and appropriate protective measures.

Within the risk management framework described in the NIPP, DHS is also responsible for the following activities:

- Providing cyber-specific expertise and assistance in addressing the cyber elements of CI/KR;
- Promoting a comprehensive national awareness program to empower businesses, the workforce, and individuals to secure their own segments of cyberspace;
- Working with security partners to reduce cyber vulnerabilities and minimize the severity of cyber attacks;
- Coordinating the development and conduct of national cyber threat assessments;
- Providing input on cyber-related issues for the National Intelligence Estimate of cyber threats to the United States;
- Facilitating cross-sector cyber analysis to understand and mitigate cyber risk;
- Providing guidance, review, and functional advice on the development of effective cyber-protective measures; and
- Coordinating cyber security programs and contingency plans, including recovery of Internet functions.

1A.2.2 Sector-Specific Agencies

Recognizing that each CI/KR sector possesses its own unique characteristics and operating models, SSAs provide the subject matter and industry expertise through relationships with the private sector to enable protection of the assets, systems, networks, and functions they provide within each of the sectors. SSAs must understand and mitigate cyber risk by:

- Identifying subject matter expertise regarding the cyber aspects of their sector;
- Increasing awareness of how the business and operational aspects of the sector rely on cyber systems and processes;
- Determining whether approaches for CI/KR inventory, risk assessment, and protective measures currently address cyber assets, systems, and networks; require enhancement; or require the use of alternative approaches;
- Reviewing and modifying existing and future sector efforts to ensure that cyber concerns are fully integrated into sector security strategies and protective activities;
- Establishing mutual assistance programs for cyber security emergencies; and
- Exchanging cyber-specific information with sector security partners, including the international community, as appropriate, to improve the Nation's overall cyber security posture.

1A.2.3 Other Federal Departments and Agencies

All Federal departments and agencies must manage the security of their cyber infrastructure while maintaining awareness of vulnerabilities and consequences to ensure that the cyber infrastructure is not used to enable attacks against the Nation's CI/KR. A number of Federal agencies have specific additional responsibilities outlined in the National Strategy to Secure Cyberspace:

- **The Department of Justice and the Federal Trade Commission:** Working with the sectors to address barriers to mutual assistance programs for cyber security emergencies.
- **The Department of Justice and Other Federal Agencies:**
  - Developing and implementing efforts to reduce or mitigate cyber threats by acquiring more robust data on victims of cyber crime and intrusions;
  - Leading the national effort to investigate and prosecute those who conduct or attempt to conduct cyber attacks;
  - Exploring means to provide sufficient investigative and forensic resources and training to facilitate expeditious investigation and resolution of CI/KR incidents; and
  - Identifying ways to improve cyber information sharing and investigative coordination among Federal, State, local, and tribal law enforcement communities; other agencies; and the private sector.
- **The Federal Bureau of Investigation and the Intelligence Community:** Ensuring a strong counterintelligence posture to deter intelligence collection against the Federal Government, as well as commercial and educational organizations.
- **The Intelligence Community, the Department of Defense, and Law Enforcement Agencies:** Improving the Nation's ability to quickly attribute the source of threats or attacks to enable timely and effective response.

1A.2.4 State, Local, and Tribal Governments

State, local, and tribal governments are encouraged to implement the following cyber recommendations:

- Managing the security of their cyber infrastructure while maintaining awareness of threats, vulnerabilities, and consequences to ensure that it is not used to enable attacks against CI/KR, and ensuring that government offices manage their computer systems accordingly;

- Participating in significant national, regional, and local awareness programs to encourage local governments and citizens to manage their cyber infrastructure appropriately; and
- Establishing cyber security programs, including policies, plans, procedures, recognized business practices, awareness, and audits.

1A.2.5 Private Sector

The private sector is encouraged to implement the following recommendations as indicated in the National Strategy to Secure Cyberspace:

- Managing the security of their cyber infrastructure while maintaining awareness of vulnerabilities and consequences to ensure that it is not used to enable attacks against the Nation's CI/KR;
- Participating in sector-wide programs to share information on cyber security;
- Evaluating the security of networks that affect the security of the Nation's CI/KR, including:
  - Conducting audits to ensure effectiveness and the use of best practices;
  - Developing continuity plans that consider the full spectrum of necessary resources, including off-site staff and equipment; and
  - Participating in industry-wide information sharing and best practices dissemination;
- Reviewing and exercising continuity plans for cyber infrastructure and examining alternatives (e.g., diversity in service providers, implementation of recognized cyber security practices) as a way of improving resiliency and mitigating risk;
- Identifying near-term R&D priorities that include programs for highly secure and trustworthy hardware, software, and protocols; and
- Promoting more secure out-of-the-box installation and implementation of software industry products, including increasing user awareness of the security features of products; ease of use for security functions; and, where feasible, promotion of industry guidelines and best practices that support such efforts.

1A.2.6 Academia

Colleges and universities are encouraged to implement several recommendations as indicated in the National Strategy to Secure Cyberspace:

- Managing the security of their cyber infrastructure while maintaining awareness of vulnerabilities and consequences to ensure that it is not used to enable attacks against the Nation's CI/KR;
- Establishing appropriate information-sharing mechanisms to deal with cyber attacks and vulnerabilities;
- Establishing an on-call point of contact for Internet service providers and law enforcement officials in the event that the institution's cyber assets, systems, or networks are discovered to be launching cyber attacks; and
- Establishing model guidelines empowering Chief Information Officers to manage cyber security, develop and exchange best practices for cyber security, and promote model user awareness programs.

1A.3 Managing Cyber Risk

Under the NIPP, risk management follows a logical process that is comprised of the following fundamental activities: (1) setting security goals; (2) identifying cyber assets, systems, networks, and functions; (3) assessing risk, which is based on consequences, threats, and vulnerability; (4) prioritizing efforts that maximize risk mitigation; (5) implementing protective programs; and (6) measuring effectiveness and improving programs. Each of these activities is discussed as they pertain to the cyber dimension of CI/KR protection in the subsections that follow.

1A.3.1 Set Security Goals

The goals and objectives set forth in the NIPP provide the overarching direction for CI/KR protection. Five cyber security objectives support the NIPP:

Objective 1: Establish a National Cyberspace Security Response System

Establishing a National Cyberspace Security Response System will improve the Nation's ability to prevent, protect against, detect, respond to, and reconstitute rapidly after a cyber incident by enhancing information exchange and analysis, improving situational awareness, and promoting collaboration and coordination among public, private, and international communities.

Section 1A.3.5 of this appendix describes various cyber security initiatives and programs, as well as exercise programs that promote effective collaborative response to cyber attack. Section 1A.4 of this appendix describes information sharing and international efforts to improve collaboration and coordination.

Objective 2: Reduce Vulnerabilities and Minimize the Severity of Cyber Attacks

Working with the public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks will help improve the security of CI/KR by reducing risks to cyber infrastructure, such as control systems.

Section 1A.3.5 of this appendix describes protective programs to reduce vulnerabilities and minimize the severity of cyber attacks.

Objective 3: Raise National Awareness of Cyber Security

Building and maintaining trusted relationships and enabling information exchange and collaboration with public, private, academic, and international partners will raise cyber security awareness. Raising national cyber security awareness, in turn, empowers businesses, the workforce, and individuals to secure their own segments of cyberspace.

Section 1A.4.1 of this appendix describes outreach and awareness initiatives to empower security partners at all levels of government and the private sector to secure cyberspace.

Objective 4: Foster Cyber Training and Education

Training and education are important components of establishing a knowledge base focused on the security of cyberspace. To foster adequate training and education to support the Nation's cyber security needs, a cadre of cyber security professionals must be developed and maintained through appropriate training and education programs.

Section 1A.4.3 of this appendix describes training and education programs designed to help develop cyber security professionals.

Objective 5: Identify and Reduce Threats to Cyberspace

Because of the ubiquitous nature of cyberspace, threats can emerge from anywhere at any time, and can be difficult to identify and track. Improving and coordinating cyber intelligence and threat detection and deterrence capabilities will help identify and reduce cyber threats.

Section 1A.4.1 of this appendix describes efforts to reduce cyber risk through improved interagency coordination.

1A.3.2 Identify Cyber Assets, Systems, Networks, and Functions

Cyber assets, systems, networks, and functions are examined as a key aspect of risk analysis. The process for identifying cyber assets, systems, networks, and functions should be repeatable, scalable, and distributable, and enable cyber interdependency analysis at both the sector and national levels to facilitate risk prioritization and mitigation.

Cyber assets, systems, and networks represent a variety of hardware and software components that perform a particular function. Examples of assets, systems, networks, and functions include networking equipment, database software, security systems, operating systems, local area networks, modeling and simulation, and electronic communications. The following are examples of cyber systems that exist in most, if not all, sectors and should be identified individually or included as a cyber element of a physical asset's description if the operation of that asset depends on them:

- **Business Systems:** Cyber systems used to manage or support common business processes and operations. Examples of business systems include Enterprise Resource Planning, e-commerce, e-mail, and R&D systems.
- **Control Systems:** Cyber systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. Control systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of control systems include SCADA, Process Control Systems, and Distributed Control Systems.
- **Access Control Systems:** Cyber systems allowing only authorized personnel and visitors physical access to defined areas of a facility. Access control systems provide monitoring and control of personnel passing throughout a facility by various means, including electronic card readers, biometrics, and radio frequency identification.

The Internet is a key resource comprised of domestic and international assets within both the Information Technology and Telecommunications sectors. It is used by all sectors to varying degrees. Availability of Internet service is the responsibility of both the Information Technology and Telecommunications sectors; however, the need for access to and reliance on the Internet are common to all sectors.

DHS, in collaboration with other security partners, provides a cross-sector cyber asset identification methodology that, when applied, enables a sector to identify cyber assets, systems, networks, and functions that may have nationally significant consequences if destroyed, incapacitated, or exploited. This methodology also characterizes the reliance of a sector's business and operational functionality on cyber assets, systems, and networks. Additional documentation on this methodology will be available in the near future. If an appropriate cyber asset identification methodology is already being used within the sector, DHS will work with the sector to ensure alignment of that methodology with the NIPP risk management framework described in chapter 3.

DHS also has ongoing efforts to ensure that the NADB and other CI/KR description databases used for risk assessment contain appropriate information on cyber assets, systems, networks, and functions.

1A.3.3 Assess Risks

Risk assessment for cyber assets, systems, and networks is an integral part of the risk management framework described in the NIPP. This framework combines consequences, threats, and vulnerabilities to produce systematic, comprehensive, and defensible risk assessments. DHS and the SSAs assess risk for cyber assets, systems, and networks associated with other CI/KR at the national and sector levels.

DHS and the SSAs will incorporate the results of these risk assessments into their overall risk management processes to prioritize where the Nation's limited resources for CI/KR protection activities should be applied.

Consequence Analysis: The first step in the risk assessment process involves determining the consequences of destruction; incapacitation; or exploitation of an asset, system, network, or the functions they provide.

To assess whether a given asset may be nationally consequential, physical, cyber, and human asset dependencies and interdependencies need to be assessed. Cyber interdependence presents a unique challenge for all sectors because of the borderless nature of cyberspace. Interdependencies are dual in nature (e.g., the Energy sector relies on computer-based control systems to manage the electric power grid, while those same control systems require electric power to operate).

Modeling and simulations through the NISAC will help quantify national and international dependency and interdependency, as well as their resulting consequences. However, this effort is highly complex and may not be appropriate for all assessments. When such advanced capability is not available or required, dependency and interdependency analyses may be carried out in a more subjective manner, with the participation of subject matter experts who have operational knowledge of the sectors involved, as well as the cross-sector interactions that are likely.

The consequences of cyber asset, system, or network destruction, incapacitation, or exploitation should be measured and described using a consistent system of measurements to ensure that the results can be compared across sectors. The NIPP provides baseline criteria for assessment methodologies to ensure such consistency. DHS also makes the RAMCAP process available for sectors to use at their discretion. While either of these approaches enables the consistent assessment of cyber consequences, both require that cyber assets, systems, networks, and functions be properly accounted for in the analysis process for the results to accurately reflect the consequences of cyber loss.

Vulnerability Assessment: The second step of the risk assessment process is analysis of vulnerability—determining which elements of infrastructure are most susceptible to attack and how attacks against these elements would most likely be carried out.

DHS works to identify cross-sector best practices to ensure that existing methodologies used by SSAs and other security partners address cyber vulnerabilities. DHS has taken a broad, inclusive approach by reviewing various existing, publicly available methods across government, industry, and academia to assemble a hybrid of the best practices. For example, DHS not only examines vulnerability standards from the International Organization for Standardization and NIST, but also studies vulnerability assessment methods used in the law enforcement and intelligence communities and the private sector.

DHS works to leverage established methodologies that have traditionally focused on physical vulnerabilities by enhancing them to better address cyber elements. Examples of these efforts include the enrichment of the Vulnerability Identification Self-Assessment Tool, as well as the RAMCAP process (see chapter 3).

There are cyber vulnerabilities that all sectors should consider when conducting their assessments, such as system interconnections. System interconnections (also known as trusted connections) are defined as the direct connection of two or more cyber systems owned by separate organizations. Business or government offices may interconnect for a variety of reasons, depending on the relationship between the interconnected entities. These interconnections may increase the security risk by exposing one system to vulnerabilities associated with another location.

Threat Analysis: The third step of the risk assessment process is the analysis of threat, which provides the likelihood that a target will be attacked. There are increasing indicators that potential adversaries intend to conduct cyber attacks and are actively acquiring cyber attack capabilities. Cyber attacks may not only target the Internet, but rather they may use it as a means of attack or for other purposes that support terrorist activities. Additionally, the increasing ease with which powerful cyber attack tools can be obtained and used puts the capability of conducting cyber attacks within reach of most groups or individuals who wish to do harm to the United States. However, credible information on specific adversaries is often not available. As such, DHS collaborates with the law enforcement and intelligence communities and the private sector to more accurately portray the possible ways in which the cyber threat may affect CI/KR, including the exploitation of the Internet as a weapon.

As called for in the National Strategy to Secure Cyberspace, DHS provides input on cyber-related issues for the National Intelligence Estimate of Cyber Threats to the U.S. Information Infrastructure. DHS will update its assessment on an annual basis to inform the general threat scenarios used in risk assessments and provide input to the National Intelligence Estimate as required.

The HITRAC conducts integrated threat analysis for CI/KR within DHS. HITRAC brings together intelligence and infrastructure specialists to ensure a complete and sophisticated understanding of the risks to U.S. CI/KR, including cyber infrastructure. To do this, HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement to integrate and analyze intelligence and law enforcement information on the threat. It also works in partnership with the SSAs and owners and operators to ensure that their expertise on infrastructure operations is integrated into threat analysis. HITRAC combines intelligence, which includes all-source information, threat assessments, and trend analysis, with expert operational and practical knowledge, and an understanding of U.S. CI/KR to provide products for CI/KR risk assessment that include actionable conclusions regarding terrorist threats and risks. Additional information on HITRAC products can be found in section 3.3.4 of the NIPP Base Plan.

1A.3.4 Prioritize

NIPP risk assessments provide comparable estimates of the risk faced by each CI/KR element and sector. This process allows key elements and sectors to be prioritized according to risk, and protective programs, including those focused on improving cyber security, to be designed that can help mitigate the highest priority risks. Those programs that offer the greatest risk mitigation for the dollars spent are afforded the highest priority. Although cyber-specific protective programs are frequently perceived to be costly, the costs of these programs may be significantly lower than the cascading costs associated with a successful cyber attack.

Cyber assets, systems, and networks and the functions they provide are prioritized using an overall risk-based approach. By integrating cyber threats, vulnerabilities, and consequences into risk analysis and by measuring risk in comparable terms for all elements and sectors, cyber assets, systems, networks, and functions are included in the prioritization process in a manner that ensures that they are appropriately considered along with other aspects of CI/KR.

1A.3.5 Implement Protective Programs

Since each sector has a unique reliance on cyber infrastructure, DHS will assist the SSAs in developing a range of effective and appropriate cyber-protective measures.

In addition to individual sector-level protective measures, DHS has partnered with other public and private sector entities to develop and implement specific programs to help improve the security of the cyber infrastructure across sectors, as well as to support national cyber risk-mitigation activities, including:

- **Government Forum of Incident Response and Security Teams (GFIRST):** Following the model of the global FIRST organization, the Federal interagency community established the GFIRST to facilitate interagency information sharing and cooperation across Federal agencies for readiness and response efforts. GFIRST is a group of technical and tactical security response team practitioners responsible for securing government information technology systems. The members work together to understand and handle computer security incidents and to encourage proactive and preventive security practices.
- **Internet Disruption Working Group:** The Internet Disruption Working Group is a strategic partnership between public and private sector entities formed in response to concerns surrounding the dependency of critical communications, operations, and services on Internet functions. In addition to relying on the Internet for communications, many CI/KR sectors rely on the Internet to transfer operational information, conduct day-to-day business transactions, and perform essential services. The Internet Disruption Working Group is focused on identifying actions that government and other security partners can take in the near term to prepare for, protect against, and mitigate nationally significant Internet disruptions. In addressing the resiliency and recovery of Internet functions, the Internet Disruption Working Group is developing trusted relationships with the private sector, including key Internet infrastructure owners and operators.
- **The National Cyber Response Coordination Group:** The NCRCG member agencies use their established relationships with the private sector and State, local, and tribal governments to facilitate cyber incident management, develop courses of action, and devise appropriate response and recovery strategies. NCRCG facilitates coordination of the Federal

Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences. Outlined in the NRP Cyber Annex, the NCRCG serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of Federal Government response and recovery efforts during a cyber crisis.

- **Programs for Federal Systems Cyber Security:** Federal prevention and protection efforts include those that are focused on securing cyber infrastructure owned and operated by the Federal Government. HSPD-7 mandates that "the heads of all Federal departments and agencies shall develop and submit to the Director of the OMB for approval plans for protecting the physical and cyber CI/KR that they own or operate. These plans address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities." To assist Federal agencies in their efforts, DHS acts as a subject matter expert to OMB in reviewing the cyber aspects of Federal agency CI/KR plans to ensure that cyber risk is addressed consistently across all Federal agencies. DHS is working with the OMB to improve Federal civilian agency cyber security practices and compliance with the Federal Information Security Management Act.

In addition to the programs listed above, DHS operates the Cyber Exercise Program in coordination with the National Exercise Program. Through this program, DHS and security partners conduct exercises to improve coordination among members of the cyber incident response community. The program includes participation from Federal, State, local, tribal, and international government elements, as well as private sector corporations, coordinating councils, and academic institutions. The main objectives of national cyber exercises are to practice coordinated response to cyber attack scenarios; provide an environment for evaluation of interagency and cross-sector processes, procedures, and tools for communications and response to cyber incidents; and foster improved information sharing among government agencies and between government and private industry.

DHS, in collaboration with other security partners, has also established several vulnerability-reduction programs under the NIPP risk management framework, including:

- **Software Assurance Program:** Public and private sector security partners work together to develop best practices and new technologies to promote integrity, security, and reliability in software development. DHS leads the Software Assurance Program, a comprehensive effort that addresses people, processes, technology, and acquisition throughout the software life cycle. Focused on shifting away from the current security paradigm of patch management, these efforts will encourage the production of higher quality, more secure software. These efforts to promote a broader ability to routinely develop and deploy trustworthy software products through public-private partnerships are a significant element of securing cyberspace and the Nation's critical infrastructure. DHS also partners with NIST in the National Information Assurance Partnership (NIAP), a Federal Government initiative originated to meet the security testing needs of both information technology consumers and producers. NIAP is operated by NSA to address security testing, evaluation, and validation programs.
- **Control Systems Cyber Security Program:** The DHS Control Systems Cyber Security Program coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors. The Control Systems Cyber Security Program coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation

Control systems, which are critical components of our Nation's critical infrastructure, monitor and control sensitive processes and functions upon which our Nation depends (e.g., electricity generation, transmission, and distribution; natural gas production and distribution; transportation systems monitoring and control; water supply and treatment; and chemical processing).

Control systems historically were designed with proprietary solutions for specific uses in isolation, but are now frequently being implemented with remote access and open connectivity, utilizing common operating systems and, thus, are potentially vulnerable to various cyber attacks. Cyber security practices commonly implemented in business systems are often difficult to implement in operational control systems environments. As a result, cyber threats to control systems could potentially have devastating impacts on national security, economic security, public health and safety, as well as the environment.

activities. These activities include assessing and managing control system vulnerabilities, assisting the US-CERT Control Systems Security Center with control system incident management, and providing control system situational awareness through outreach and training initiatives.

- **The Standards and Best Practices Program:** As part of its efforts to develop practical guidance and review tools, and promote R&D investment in cyber security, DHS and NIST co-sponsor the National Vulnerability Database. This database provides centralized and comprehensive vulnerability mitigation resources for all types of users, including the general public, system administrators, and vendors to assist with incident prevention and management (including links to patches) to mitigate consequences and vulnerabilities.

1A.3.6 Measure Effectiveness and Improve Programs

There are several core cyber measures and metrics that will be tracked within and across sectors to enable comparison and analysis between and among different types of critical infrastructure. DHS will work with security partners to develop descriptive, process, and outcome cyber core metrics to enable realistic evaluation of cyber security within and across sectors. The cyber core measures and metrics will parallel those being developed for the NIPP, and will also include the review, consideration, and integration of common cyber security policies, plans, procedures, and sound business practices, as appropriate. Separate sector-specific measures for cyber security may not be necessary in all cases; however, the sector-specific measures should strive to consider all sector assets, including cyber assets, systems, networks, and functions when measuring performance against goals.

Once the cyber core metrics have been developed and approved, DHS will establish a data-gathering and reporting process in cooperation with SSAs and other security partners to measure progress. This process will outline, but will not be limited to, the responsible parties, data collection and reporting methodology, and timeframes for data and metrics submissions. Additionally, as the process matures, additional metrics will be considered to reflect the most important issues currently being faced by the sectors.

The overall purpose of measuring effectiveness using metrics is to improve cyber CI/KR protection by mitigating risk. This means that using metrics as descriptors is not sufficient and that measured effectiveness must be compared to goals and improvements to enable the addressing of priority gaps.

1A.4 Ensuring Long-Term Cyber Security

The effort to ensure a coherent cyber CI/KR protection program over the long term has four components that are described in greater detail below:

- **Information Sharing and Awareness:** Ensures implementation of effective, coordinated, and integrated protection of cyber assets, systems, and networks, and the functions they provide, and enables cyber security partners to make informed decisions with regard to short- and long-term cyber security postures, risk mitigation, and operational continuity.
- **International Cooperation:** Promotes a global culture of cyber security and improves overall cyber incident preparedness and response posture.
- **Training and Education:** Ensures that skilled and knowledgeable cyber security professionals are available to undertake NIPP programs in the future.
- **Research and Development:** Improves cyber security protective capabilities or dramatically lowers the costs of existing capabilities so that State, local, tribal, and private sector security partners can afford to do more with their limited budgets.

1A.4.1 Information Sharing and Awareness

Information sharing and awareness involves sharing programs with agency partners and other security partners, and special sharing arrangements for emergency situations. Each of these is discussed below:

Interagency Coordination: Interagency cooperation and information sharing are essential to improving national cyber counterintelligence and law enforcement capabilities. The intelligence and law enforcement communities have both official and informal mechanisms in place for information sharing that DHS supports:

- **FBI's Cyber Task Forces** involve more than 50 law enforcement agency cyber task forces and more than 80 additional cyber working groups throughout the country, collaborating with Federal, State, and local partners to maximize investigative resources to ensure a timely and effective response to cyber security threats of both a criminal and national security nature.
- **Cybercop Portal** is a secure Internet-based information-sharing mechanism for more than 5,300 law enforcement members involved in the field of electronic crimes investigations. The law enforcement community, including investigators from private industry (e.g., banks and the network security community), is tied together and supported by this secure, Internet-based collaboration portal.
- **FBI's InfraGard** program is a public-private partnership coordinated out of the 56 FBI field offices nationwide. The program brings together law enforcement, academia, and private sector entities on a monthly basis to provide a forum for information sharing and networking.
- **FBI's Inter-Agency Coordination Cell** is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
- **U.S. Secret Service's Electronic Crimes Task Forces** provide interagency coordination on cyber-based attacks and intrusions.

Information Sharing and Analysis Centers: Underscoring effective cyber security efforts is the importance of information sharing between and among industry and government. To this end, the Information Technology and Communications ISACs work closely together and with DHS and the SSAs to maximize resources, coordinate preparedness and response efforts, and maintain situational awareness to enable risk mitigation regarding cyber infrastructure.

Cyber Security Awareness for Security Partners: DHS plays an important leadership role in coordinating a public-private partnership to promote and raise cyber security awareness among the general public by:

- Partnering with other Federal and private sector organizations to sponsor the National Cyber Security Alliance (NCSA), including creating a public-private organization, Stay Safe Online, to educate home users, small businesses, and K-12 and higher education audiences on cyber security best practices.
- Engaging with the MS-ISAC to help enhance the Nation's cyber security readiness and response at the State and local levels, and launching a national cyber security awareness effort in partnership with the MS-ISAC. The MS-ISAC is an information-sharing organization, with representatives of State and local governments, that analyzes, sanitizes, and disseminates information pertaining to cyber events and vulnerabilities to its constituents and private industry.
- Collaborating with the NCSA, the MS-ISAC, and the public and private sector to establish October as National Cyber Security Awareness Month and participating in activities to continuously raise cyber security awareness nationwide.

Cyberspace Emergency Readiness: DHS established the US-CERT, which is a 24/7 single point of contact for cyberspace analysis and warning, information sharing, and incident response and recovery for a broad range of users, including government, enterprises, small businesses, and home users. US-CERT is a partnership between DHS and the public and private sectors designed to help secure the Nation's Internet infrastructure and to coordinate defenses against and responses to cyber attacks across the Nation. US-CERT is responsible for:

- Analyzing and reducing cyber threats and vulnerabilities;
- Disseminating cyber threat warning information; and
- Coordinating cyber incident response activities.

To support the information-sharing requirements of the network approach, US-CERT provides the following information on their Web site, accessible via the HSIN, and via mailing lists:

- **Cyber Security Alerts:** Written in a language for home, corporate, and new users, these alerts are published in conjunction with technical alerts in the context of security issues that affect the general public.
- **Cyber Security Bulletins:** Bulletins summarize information that has been published regarding emergent security issues and vulnerabilities. They are published weekly and are written primarily for systems administrators and other technical users.
- **Cyber Security Tips:** Tips provide information and advice on a variety of common cyber security topics. They are published biweekly and are written primarily for home, corporate, and new users.
- **National Web Cast Initiative:** In an effort to increase cyber security awareness and education among the States, DHS, through US-CERT, and the MS-ISAC have launched a joint partnership to develop a series of national Web casts that will examine critical and timely cyber security issues. The purpose of the initiative is to strengthen the Nation's cyber readiness and resilience.
- **Technical Cyber Security Alerts:** Written for systems administrators and experienced users, technical alerts provide timely information on current cyber security issues, vulnerabilities, and exploits.

US-CERT also provides a method for citizens, businesses, and other institutions to communicate and coordinate directly with the Federal Government on matters of cyber security. The private sector can use the protections afforded by the Protected Critical Infrastructure Information Act to electronically submit proprietary data to US-CERT.

1A.4.2 International Coordination on Cyber Security

The Federal Government proactively uses its intelligence capabilities to protect the country from cyber attack, its diplomatic outreach and operational capabilities to build partnerships in the global community, and its law enforcement capabilities to combat cyber crime wherever it originates. The private sector, international industry associations, and companies with global interests and operations are also engaged in addressing cyber security internationally. For example, the U.S.-based Information Technology Association of America participates in international cyber security conferences and forums, such as the India-based National Association for Software and Service Companies Joint Conference. These efforts involve interaction with both the policy and operational communities to coordinate national and international activities that are mutually supportive across the globe:

- **International Cyber Security Outreach:** DHS, in conjunction with the Department of State and other Federal agencies, engages in multilateral and bilateral discussions to further international security awareness and policy development, as well as incident response team information-sharing and capacity-building objectives. The United States engages in bilateral discussions on important cyber security issues with close allies and others with whom the United States shares networked interdependencies, to include, but not limited to: Australia, Canada, Egypt, Germany, Hungary, India, Italy, Japan, the Netherlands, Romania, the United Kingdom, etc. The United States also provides leadership in multilateral and regional forums addressing cyber security and CI/KR protection to encourage all nations to take systematic steps to secure their networked systems. For example, U.S. initiatives include: the Asia-Pacific Economic Cooperation Telecommunications Working Group capacity-building program to help member countries develop CSIRTs, and the OAS framework proposal to create a regional computer incident response points-of-contact network for information sharing and to help member countries develop CSIRTs. Other U.S. efforts to build a culture of cyber security include participation in OECD, G8, and

United Nations activities. The U.S. private sector is actively involved in this international outreach in partnership with the Federal Government.

- **Collaboration on Cyber Crime:** The U.S. outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe Convention on Cyber Crime, as well as: (1) the G8 High-Tech Crime Working Group's principles for fighting cyber crime and protecting critical information infrastructure, (2) the OECD guidelines on information and network security, and (3) the United Nations General Assembly resolutions based on the G8 and OECD efforts. The goal of this outreach strategy is to encourage individual nations and regional groupings of nations to join DHS in efforts to protect internationally interconnected national systems.
- **Collaborative Efforts for Cyber Watch, Warning, and Incident Response:** The Federal Government is working strategically with key allies on cyber security policy and operational cooperation. For example, DHS is leveraging pre-existing relationships among CSIRTs. DHS also has established a preliminary framework for cooperation on cyber security policy, watch, warning, and incident response with key allies. The framework also incorporates efforts related to key strategic issues as agreed upon by these allies. An IWWN is being established among cyber security policy, computer emergency response, and law enforcement participants representing 15 countries. The IWWN will provide a mechanism for the participating countries to share information to build global cyber situational awareness and coordinate incident response.
- **Partnerships to Address Cyber Aspects of Critical Infrastructure Protection:** DHS and the SSAs are leveraging existing agreements, such as the SPP and the JCG with the United Kingdom, to address the Information Technology sector and cross-cutting cyber components of CI/KR protection. The trilateral SPP builds on existing bilateral agreements between the United States and Canada and the United States and Mexico by allowing issues to be addressed on a dual bi-national basis. In the context of the JCG, DHS established a 10-point action plan to address cyber security, watch, warning, and incident response and other strategic initiatives.

1A.4.3 Training and Education

The National Strategy to Secure Cyberspace highlights the importance of cyberspace security training and education. Education and training are strategic initiatives in which DHS and other Federal agencies are actively engaged to affect a greater awareness and participation in efforts to promote cyber security for the future.

The Federal Government has undertaken several initiatives in partnership with the research and academic communities to better educate and train future cyber security practitioners:

- DHS co-sponsors the National CAEIAE program with NSA. Together, DHS and NSA are working to expand the program nationally.
- DHS collaborates with the National Science Foundation to co-sponsor and expand the Cyber Corps Scholarship for Service program. The Scholarship for Service program provides grant money to selected CAEIAE and other universities with programs of a similar caliber to fund the final 2 years of bachelor's, master's, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal Government.
- In fiscal year 2004, the joint DHS/Treasury Computer Investigative Specialist program trained 48 Federal criminal investigators in basic computer forensics. Agents from ICE, the Internal Revenue Service, and the U.S. Secret Service attended the basic 6½-week course. This training was funded through the Treasury Executive Office of Asset Forfeiture.
- DHS is collaborating with DOD to finalize a comprehensive information technology job skills standard to guide development of a national certification program for security professionals within the Federal Government and private industry.
- Through DHS, DOJ, DOD, and the Department of State, the Federal Government provides cyber-related training to foreign cyber incident responders (incident response management, creation of CSIRTs) and law enforcement personnel and jurists (laws, computer forensics, case handling).

1A.4.4 Research and Development

The Cyber Security Research and Development Act of 2002 authorized a multi-year effort to create more secure cyber technologies, expand cyber security R&D, and improve the cyber security workforce.

To further address cyber R&D needs, the White House's OSTP established a CSIA IWG under the NSTC. The CSIA IWG was jointly chartered by NSTC's Subcommittee on Networking and Information Technology R&D and the Subcommittee on Infrastructure. This interagency working group includes participation from 20 organizations representing 11 departments and agencies, as well as from several offices in the White House.

The purpose of the working group is to coordinate Federal programs for cyber security and information assurance R&D. It also is responsible for developing the Federal Plan for Cyber Security and Information Assurance R&D, which includes near-term, mid-term, and long-term cyber security research efforts in response to the National Strategy to Secure Cyberspace and HSPD-7. The document includes descriptions of approximately 50 cyber security R&D topics, such as Automated Attack Detection, Warning, and Response; Forensics, Traceback, and Attribution; Security Technology and Policy Management Methods; Policy Specification Languages; and Integrated, Enterprise-Wide Security Monitoring and Management. The document also identifies the top cyber security and information assurance research topics across the Federal Government. Finally, the document includes key findings and recommendations. DHS actively co-chairs the CSIA IWG with OSTP and continues to identify critical cyber R&D requirements for incorporation into Federal R&D planning efforts.

1A.4.5 Exploring Private Sector Incentives

Awareness and understanding of the need for cyber security present a challenge for both government and industry. Although cyber security requires significant investments in time and resources, an effective cyber security program may reduce the likelihood of a successful cyber attack or the impact if a cyber attack occurs. Network disruptions resulting from cyber attacks can lead to loss of money, time, products, reputation, sensitive information, or even potential loss of life through cascading effects on critical systems and infrastructure. From an economic perspective, cyber attacks have resulted in billions of dollars of business losses and damages in the aggregate.

The private sector makes risk management decisions, including those for cyber security, based on return on investment and ensuring business continuity. Market-based incentives for cyber security investments include protection of intellectual capital, security-influenced procurement, market differentiation, and public confidence. Sometimes, however, cyber assets, systems, networks, or functions may be deemed nationally critical and necessitate additional risk management beyond that which the private sector implements as part of their corporate responsibility. To address this difference, DHS is collaborating with the public and private sectors through various programs and outreach efforts (e.g., US-CERT, the Control Systems Cyber Security Program, and the Software Assurance Program) to promote awareness of cyber security risks, and create incentives for increased investment in cyber security.

Appendix 1B: International CI/KR Protection

1B.1 Introduction and Purpose of This Appendix

This appendix provides guidance for addressing the international aspects of CI/KR protection in support of the NIPP.

1B.1.1 Scope

The NIPP provides the mechanisms, processes, key initiatives, and milestones necessary to enable DHS, the Department of State, the SSAs, and other security partners to address international implications and requirements related to CI/KR protection. The NIPP and associated SSPs recognize that protective measures do not stop at a facility's fence line or a national border. Because disruptions in the global infrastructure can ripple and cascade around the world, the NIPP and SSPs also must consider cross-border CI/KR, international vulnerabilities, and global dependencies and interdependencies.

1B.1.2 Vision

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets identifies "fostering international cooperation" as one of the eight guiding principles of its vision for the future. The strategy underscores the need for a coordinated, comprehensive, and aggressive global action as a key aspect of the NIPP approach to CI/KR protection.

Furthermore, the National Strategy to Secure Cyberspace sets forth strategic objectives for national security and international cyberspace security cooperation that deal directly with the international aspects of CI/KR protection, including preventing cyber attacks against America's critical infrastructure, reducing vulnerabilities, and minimizing damage and recovery time from cyber attacks and incidents that do occur.

1B.1.3 Implementing the Vision With a Strategy for Effective Cooperation

The NIPP CI/KR international coordination and protection strategy outlined in this appendix is focused on instituting effective *cooperation with international security partners*, rather than on discussing *specific protective measures*. Specific protective measures are tailored to each sector's particular circumstance and are developed in the SSPs. This appendix also focuses on implementing existing agreements that affect CI/KR protection and addressing cross-sector and global issues such as cyber security.

The Department of State, DHS, and the SSAs will periodically review the international CI/KR protection strategy and redraft it, as needed, to ensure that it complements and supports specific objectives detailed in the NIPP.

Within 6 months of the approval of the NIPP, DHS, the Department of State, and other concerned Federal agencies will incorporate the NIPP into their strategies for cooperating with other countries and international/multinational organizations. This effort will focus on promoting a global culture of physical and cyber security, managing CI/KR-related risk as far as possible outside the physical borders of the United States; accelerating international cooperation to develop intellectual infrastructure based on shared assumptions and compatible conceptual tools; and connecting constituencies not traditionally engaged in security. The broad structure of this approach is outlined in this appendix; it is based on the following high-level considerations.

1B.2 Responsibilities for International Cooperation on CI/KR Protection

In accordance with HSPD-7, the Department of State, in conjunction with DHS, DOJ, DOD, the Departments of Commerce and Treasury, the NRC, and other appropriate agencies, is responsible for working with foreign countries and international/multinational organizations to strengthen the protection of U.S. CI/KR. This section provides further details regarding the responsibilities of DHS and other security partners related to the international dimension of CI/KR protection.

1B.2.1 Department of Homeland Security

Under the CI/KR risk management framework described in this plan, DHS, in collaboration with other security partners, is responsible for the following actions, all of which have an international dimension:

- Building security partnerships;
- Implementing a comprehensive, integrated risk management program; and
- Implementing protective programs.

DHS, in conjunction with the Department of State and in cooperation with other foreign affairs agencies, will share with international entities appropriate information and perform outreach functions to enhance information sharing and management of international agreements regarding CI/KR protection.

Some of the more complex challenges presented by the international aspects of CI/KR protection involve analyzing the complex dependencies, interdependencies, and vulnerabilities that require the application of sophisticated and innovative modeling techniques. DHS is responsible for pursuing research and analysis in this area. It will call on a range of outside sources for this work, including those with expertise in the international community and the NISAC.

1B.2.2 Department of State

The Secretary of State has direct responsibility for policies and activities related to the protection of U.S. citizens and U.S. facilities abroad. The Secretary of State, in conjunction with the Secretary of Homeland Security, is responsible for coordinating with foreign countries and international organizations to strengthen the protection of U.S. CI/KR. The Department of State supports DHS and other Federal agency efforts by providing knowledge about and access to other governments. The Department of State

leverages bilateral and multilateral relationships around the world to ensure that the Federal Government can act effectively to identify and protect U.S. CI/KR.

The Department of State, DHS, and other agencies are engaged in a wide range of activities throughout the world to prevent, disrupt, and deter threats and acts of terrorism directed against the homeland and U.S. interests abroad. The objectives of these efforts are to develop and work with global partners to ensure mutual security and to raise awareness of the terrorist threat.

1B.2.3 Other Federal Agencies

SSAs exchange information, including cyber-specific information, with security partners in other countries, in accordance with guidelines established by DHS and the Department of State and other agencies, as appropriate, to improve the Nation's overall CI/KR protection posture.

The Departments of Commerce and Treasury, DOJ, DOD, DOE, DOT, and other agencies share responsibility, in accordance with HSPD-7, for working through the Department of State to reach out to foreign countries and international organizations to strengthen the protection of U.S. CI/KR.

1B.2.4 State, Local, and Tribal Governments

State, Territorial, local, and tribal governments ensure ongoing cooperation with relevant international, regional, local, and private sector CI/KR protection efforts.

1B.2.5 Private Sector

DHS is working with the private sector, SSAs, private voluntary and nongovernmental organizations, and information-sharing mechanisms and organizations to protect cross-border infrastructure and understand international and global vulnerabilities. DHS relies on the private sector for data, expertise, and knowledge of their international operations to identify relevant international assets, systems, and networks, and assess risks and global vulnerabilities, including shared threats and interdependencies.

1B.2.6 Academia

The academic community provides data, insight, and research into the significance of international interdependencies, modeling, and analysis.

1B.3 Managing the International Dimension of CI/KR Risk

The NIPP addresses international CI/KR protection, including interdependencies and the vulnerability to threats that originate outside the country. The NIPP brings a new focus to international security cooperation and provides a risk-based strategic framework for measuring the effectiveness of international CI/KR protection activities. The NIPP also provides tools to assess international vulnerabilities and interdependencies that complement long-standing cooperative agreements with Canada, Mexico, the United Kingdom, NATO, and others, and provides a framework for effective collaborative engagement with additional international partners.

SSPs are required to include international considerations as an integral part of each sector's planning process rather than instituting a separate layer of planning. Some international aspects of CI/KR protection require additional overarching or cross-sector emphasis. These include:

- U.S. interaction with foreign governments and international organizations to enhance the confidentiality, integrity, and availability of cyber-based infrastructure that often has an international or even global dimension;

- Protection of physical assets located on, near, or extending across the borders with Canada and Mexico that require cooperation with and/or planning and resource allocation among neighboring countries, States bordering on these countries, and affected local and tribal governments;
- Sectors with CI/KR that are extensively integrated into an international or global market (e.g., Banking and Finance or other information-based sector, Energy, or Transportation) or when the proper functioning of a sector relies on inputs that are not within the control of U.S. entities; and
- U.S. Government and corporate facilities located overseas that may be regarded as CI/KR may be determined to be critical based on implementation of the NIPP framework. Protection for the Government Facilities sector involves careful interagency collaboration, as well as cooperation with foreign CI/KR security partners.

The following subsections discuss issues associated with the international aspects of CI/KR protection in the context of the steps of the NIPP risk management process. (See NIPP Chapter 3, The Protection Program Strategy: Managing Risk.)

1B.3.1 Setting Security Goals

The overarching goal of the NIPP—to enhance the protection of U.S. CI/KR—applies to the international "system of systems" that underpins U.S. CI/KR. The NIPP and the SSPs provide guidance and risk management approaches that address the international aspects of CI/KR protection efforts on both a national and a sector-specific basis. In addition, a separate set of goals and priorities guide cross-sector efforts to improve protection for CI/KR with international linkages. These goals fall into three categories:

- Identifying and addressing cross-sector and global issues;
- Implementing existing and developing new agreements that affect CI/KR; and
- Improving the effectiveness of international cooperation.

DHS, in conjunction with the Department of State and other security partners, will define the requirement for a comprehensive international CI/KR protection strategy. The integration of international CI/KR protection considerations and measures into the SSPs is important for pursuing and achieving these goals in ways that complement each other and are achievable with the resources available.

Important considerations in achieving these goals are discussed in this section; actions required to achieve these goals are addressed in the section on key implementation actions.

1B.3.2 Identifying CI/KR Affected by International Linkages

Once international security goals are set, the next step in the risk management process is to develop and maintain a comprehensive inventory of the Nation's CI/KR outside U.S. borders and of foreign CI/KR that may affect systems within this country. The process for identifying nationally critical CI/KR involves working with U.S. industry, SSAs, academia, and international partners to gather and protect information on the foreign infrastructure and resources on which U.S. CI/KR rely.

Dependency and Interdependency and International CI/KR Protection Cooperation: The NIPP risk management framework details a structured approach for use in determining dependencies and interdependencies, including physical, cyber, and international considerations. This approach is designed to address CI/KR protection in three areas:

- Direct international linkages to physical and cyber U.S. CI/KR:
  - Foreign cross-border assets linked to U.S. CI/KR, such as roads, bridges, pipelines, gas lines, telecommunications lines and undersea cables and facilities, and power lines, etc., physically connecting U.S. CI/KR to Canada and Mexico;

  - Foreign infrastructure whose disruption or destruction could directly harm the U.S. homeland, such as waters behind a Canadian dam that could flood U.S. territory or a toxic plume from an impacted Mexican chemical plant that could contaminate U.S. territory, or foreign ports where security failures could directly affect U.S. security; and
  - U.S. CI/KR that may be located overseas, such as non-military government facilities, are overseas components of U.S. CI/KR;
- Indirect international linkages to physical and cyber U.S. CI/KR:
  - The potential cascading and escalating effects of disruption or destruction of foreign assets, systems, and networks; critical foreign technology; goods; resources; transit routes; and chokepoints; and
  - Foreign ownership, control, or involvement in U.S. CI/KR and related issues; and
- Global aspects of physical and cyber U.S. CI/KR:
  - Assets, systems, and networks either located around the world or with global mobility that require the efforts of multiple foreign countries to secure.

Dependency and interdependency analysis is primarily based on information from each sector and is formulated by the judgments of CI/KR owners and operators regarding their supply chains and sources of services from other infrastructure sectors, such as Energy and Water. As the capability for sophisticated network analysis grows, these inputs will be complemented by assessments that examine less apparent network-based dependencies and interdependencies. The NISAC supports this effort by analyzing and quantifying national and international dependency and interdependency for complex systems and networks that affect specific sectors.

1B.3.3 Assessing Risks

The risk assessment for CI/KR assets, systems, and networks that are affected by international linkages is an integral part of the risk management framework described in the NIPP. The risk management framework combines consequences, threats, and vulnerabilities to produce systematic and comprehensive risk assessments that can be clearly explained in a three-step process:

- Determining the consequences of destruction, incapacitation, or exploitation of an asset, system, or network. This is done to assess potential national significance, as well as physical, cyber, and human dependencies and interdependencies that may result from international linkages.
- Analyzing vulnerability, including determining which elements of CI/KR are most susceptible to attack or other disruption, and whether attacks against these elements could be a consequence of any international linkages.
- Conducting a threat analysis that provides the likelihood that a target will be attacked. CI/KR with international linkages may present greater opportunities for attack and thus increase the likelihood that they may be the subject of attacks.

Issues important to the other countries may be different from those for the United States. Risk analysis needs to be conducted in coordination with other countries in order to draw on their analysis, as well as our own.

1B.3.4 Prioritizing

Assessing CI/KR on a level playing field that adjudicates risk based on a common framework ensures that resources are applied where they offer the most benefit for reducing risk; deterring threats; and minimizing the consequences of attacks, natural disasters, and other emergencies. The same prioritization used for domestic CI/KR protection is observed to evaluate the risk arising from international linkages. The priority for protection investments could be raised if international linkages increase the risk.

1B.3.5 Implementing Programs

The SSAs have primary responsibility for developing protective measures that address risks that arise from international factors. In addition to sector protective measures, DHS has specific programs to help enhance the cooperation and coordination needed to address the unique challenges posed by the international aspects of CI/KR protection:

- **International Outreach Program:** DHS works in conjunction with the Department of State and with other foreign affairs agencies to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of organizational and policymaking structures, information-sharing mechanisms, industry partnerships, best practices, training, and other programs as needed to improve the protection of overseas assets and the reliability of foreign infrastructure on which the United States depends.
- **The National Cyber Response Coordination Group:** The NCRCG facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences (collectively known as cyber incidents). It serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of Federal Government response and recovery efforts during a cyber incident. The NCRCG considers and consults with international partners on a regular basis for routine situational awareness and during incidents. NCRCG member agencies integrate their capabilities to facilitate assessment of the domestic and international scope and severity of a cyber incident.
- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP. The exercise program, as appropriate, engages international partners to address cooperation and cross-border issues, including those related to CI/KR protection. DHS and other security partners also participate in exercises sponsored by international partners, including cross-border, multi-sector tabletops.
- **National Cyber Exercises:** DHS is conducting exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, Territorial, local, tribal, and international government elements, as well as private sector corporations and coordinating councils.

Because of the complex nature of the international dimension of CI/KR, a substantial emphasis is placed on best practices that can be used to improve cooperation and coordination. To this end, DHS will lead efforts to:

- Collaborate to establish global best practices, successful protection measures, and best practices related to telecommunications, air transportation systems, container shipping, cyber security, and other global systems as appropriate;
- Encourage the development and adoption of, and adherence to, standards of the International Organization for Standards and similar organizations that can help to reduce insurance premiums and level CI/KR protection costs for businesses; and
- Work with international security partners to determine the appropriate threshold for engagement with countries on cyber issues.

1B.3.6 Measuring Effectiveness and Making Improvements

The NIPP specifies three types of quantitative indicators to measure program effectiveness:

- **Descriptive Metrics** are necessary to understand sector resources and activities; they do not reflect CI/KR protection performance;
- **Process Metrics** measure whether specific activities were performed as planned; these track the progression of a task or report on the completion of an enabling process, such as forming a bilateral partnership; and
- **Outcome Metrics** track progress toward a strategic goal by beneficial results rather than level of activity.

The NIPP also distinguishes between two groups of metrics: core metrics that enable comparison and analysis between and among different sectors and sector-specific metrics that are useful within a sector.

Because protective measures are designed, implemented, and evaluated through sector-specific mechanisms guided by the SSPs, they deal with the protection challenges for a particular facility, network, or sector rather than international issues that may affect protection measures. Conversely, most initiatives that address the international issues affecting CI/KR protection are enablers rather than protective measures themselves. As a result, the metrics used to measure the effectiveness of international CI/KR protection initiatives will primarily be process metrics in the core group of CI/KR protection metrics. These will measure progress on tasks that enable CI/KR protection in situations that have international ramifications.

These metrics will be used to manage the comprehensive international CI/KR protection strategy, which enables SSP protection initiatives, and to track progress toward the strategy's three goals:

- Improving the effectiveness of international cooperation;
- Implementing existing and developing new agreements that affect CI/KR; and
- Addressing cross-sector and global CI/KR protection issues.

DHS, in cooperation with other Federal agencies, will develop the metrics to track progress on international CI/KR protection enablers. Examples of such metrics include:

- The international issues being faced by each sector, which of these affect multiple sectors, and which issues are the most important;
- The countries that should be involved in protection partnerships for each sector;
- The number and type of bilateral and multinational agreements affecting CI/KR protection;
- The nature, level of implementation, and effectiveness of bilateral and multinational agreements;
- The sectors affected by each international partnership;
- The number and type of outcomes enabled by an international initiative; and
- Where possible, the specific CI/KR protection enhancements that are directly attributable to a particular international initiative.

Once the core metrics have been developed and approved, DHS, the SSAs, and other security partners will collaborate to establish a data-gathering and reporting process. This process will outline, but will not be limited to, responsibilities; data collection, reporting procedures, and timeframes; metrics calculation; and the schedule for computing and updating the metrics on a regular basis.

1B.4 Organizing International CI/KR Protection Cooperation

DHS, in conjunction with the Department of State and other Federal agencies, works with individual foreign governments, and regional and international organizations in partnership to enhance the protection of the Nation's CI/KR and to deny the exploitation of CI/KR assets. Potential partnerships depend on:

- Physical proximity to the United States or U.S. assets;
- Useful experience and information to be gained from other countries;
- Existing alliances, agreements, and high-level commitments;

- Critical supply chains and vulnerable nodes; and
- Interdependencies and networked technologies, and the need for a global "culture of security" to protect physical, cyber, and human assets.

As international CI/KR protection partnerships mature, cooperative efforts will strengthen in two dimensions:

- Development of new partnerships with countries possessing useful experience and information regarding CI/KR protective efforts, as well as terrorism prevention, preparedness, response, and recovery; and
- Development of new international relationships and institutions to protect global infrastructure and address international interdependencies, networked technologies, and the need for a global culture of physical and cyber security.

The coordination mechanisms supporting the NIPP create linkages between CI/KR protection efforts at the national, sector, State, regional, local, tribal, and international levels. The entities and bodies that are involved with this coordination are diverse and depend on the specifics of the issues they address, as well as other considerations as discussed in the following subsections.

1B.4.1 Domestic Aspects of International CI/KR Protection Cooperation

Interagency Coordination—Department of State and DHS Leadership: DHS will work with the Department of State, international partners, and with U.S. entities involved with the international aspects of CI/KR protection to exchange experiences, share information, and develop a cooperative atmosphere to materially improve U.S. CI/KR protection, information sharing, cyber security, and global telecommunications standards. DHS and SSAs will work with specific countries to identify international interdependencies and vulnerabilities. SSAs will consider such international factors as cross-border infrastructure, international vulnerabilities, and global interdependencies in their SSPs.

Interagency Coordination—Review of Existing Mechanisms to Support the NIPP: The International Affairs offices in Federal Government agencies maintain existing relationships with foreign counterpart ministries and agencies, and are the primary partners with the Department of State in coordinating with foreign governments on international CI/KR matters.

DHS also works with SSAs to ensure that SSPs reflect international factors, such as cross-border infrastructure, international interdependencies, and global vulnerabilities.

The Department of State presently chairs an interagency working group that coordinates U.S. international CI/KR protection outreach activities. Within 30 days of publication of this plan, the Department of State and DHS will review the working group's charter and its coordination mechanisms to ensure that they address all international CI/KR issues specified by the NIPP. The Department of State and DHS, in coordination with other interagency working group members, will, within an additional 30 days, implement any changes needed to ensure that all NIPP requirements will be met and that the working group's charter reflects a role that best supports the comprehensive international CI/KR protection strategy.

1B.4.2 Foreign Aspects of International CI/KR Protection

International cooperation on cyber security and other CI/KR protection issues (e.g., energy supplies) of a global nature is necessary because of the cross-border or borderless nature of these infrastructures. These efforts require interaction on both the policy and the operational levels and involve a broad range of entities from both the government and the private sector. Interaction on the international aspects of CI/KR protection takes place bilaterally, regionally, and multilaterally:

- **Bilateral:** DHS, in conjunction and consultation with the Department of State, participates in bilateral discussions and programs with countries of interest where issues are best addressed on a country-to-country basis.
- **Regional:** DHS and the Department of State partner together to provide leadership in regional groups, such as the OAS and the Asia-Pacific Economic Cooperation, to raise awareness and develop cooperative programs.

The United States engages with Canada and Mexico, as regional neighbors, on CI/KR protection to enhance collaboration efforts. Current activities include the United States, Canada, and Mexico trilateral SPP; the U.S.-Canada Critical Infrastructure Protection Framework for Cooperation (Smart Border Action Plan); and the U.S.-Mexico Critical Infrastructure Protection Framework for Cooperation (Border Partnership Action Plan).

- **Multilateral:** Multilateral collaboration on this aspect of CI/KR involves initiatives on the part of the OECD, G8, and United Nations. For the cyber security aspects of global CI/KR protection, DHS has established a preliminary framework for cooperation on cyber security policy, watch and warning, and incident response for CI/KR with key allies such as Australia, Canada, New Zealand, and the United Kingdom. DHS is coordinating and participating in the establishment of an IWWN among cyber security policy, computer emergency response, and law enforcement participants of 15 countries. The IWWN will provide a mechanism for the participating countries to share information to build cyber situational awareness and coordinate incident response.

1B.4.3 Working With Specific Countries and International Organizations

DHS, SSAs, and other security partners will work with other countries to promote CI/KR protection best practices and they will pursue infrastructure security through international/multinational organizations such as the G8, NATO, European Union, OAS, OECD, and Asia-Pacific Economic Cooperation. The approach to working with some specific countries and organizations is founded on formal agreements that address cooperation on CI/KR protection.

- **Canada and Mexico:** The CI/KR relationships between the United States and its immediate neighbors make the borders virtually transparent. Electricity, natural gas, oil, telecommunications, roads, rail, food, water, minerals, and finished products cross the borders on a regular basis as part of normal commerce. The importance of this trade, and the infrastructure that supports it, was highlighted after the terrorist attacks of September 11, 2001, nearly closed both borders. The United States entered into the 2001 Smart Border Declaration with Canada and the 2002 Border Partnership Declaration with Mexico, in part, to address bilateral CI/KR issues. In addition, the 2005 SPP established a trilateral approach to common security issues. The SPP is based on the principle that the prosperity of all three nations is dependent on mutual security. The SPP complements, rather than replaces, existing agreements.
- **United Kingdom:** The United Kingdom is a close ally with much experience in fighting terrorism and protecting its CI/KR. The United Kingdom has developed substantial expertise in law enforcement and intelligence systems, and in the protection of commercial facilities based on its experience in countering terrorism. Like the United States, most of the critical infrastructure in the United Kingdom is under private management. The government of the United Kingdom has developed an effective, sophisticated system of managing public-private partnerships. DHS has formed a JCG with the United Kingdom that brings officials into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.
- **G8:** In the recent terrorist attacks against the United States, Spain, and the United Kingdom, the infrastructure in G8 countries was exploited and used to inflict casualties and fear. The G8 has underscored its determination to combat all forms of terrorism and to strengthen international cooperation. Counterterrorism work has been the focus of a number of initiatives launched at recent summits. At their meeting in Gleneagles Hotel in Scotland, in July 2005, the G8 heads of government issued a Statement on Counter-Terrorism. In it, they pledged to "commit ourselves to new joint efforts. We will work to improve the sharing of information on the movement of terrorists across international borders, to assess and address the threat to the transportation infrastructure, and to promote best practices for rail and metro security." DHS will work closely with the G8 to address the common threats to CI/KR and cyberspace.
- **European Union:** The European Union is pursuing CI/KR as a matter of policy, noting that an effective strategy should focus on both preparedness and on consequence management. DHS will engage the European Union early in this process to share its experience, and to further cooperate on characteristics and common vulnerabilities of critical infrastructure and cyberspace, risk analysis techniques, and strategies to mitigate risk and minimize consequences.

- **North Atlantic Treaty Organization:** NATO addresses CI/KR issues through the Senior Civil Emergency Planning Committee, the senior policy and advisory body to the North Atlantic Council on civil emergency planning and disaster relief matters. The committee is responsible for policy direction and coordination of Planning Boards and Committees in the NATO environment. It has developed considerable expertise that applies to CI/KR protection and has planning boards and committees covering ocean shipping, inland surface transport, civil aviation, food and agriculture, industrial preparedness, civil communications planning, civil protection, and civil-military medical issues. DHS has a delegation to the Senior Civil Emergency Planning Committee at NATO, participates in NATO's telecommunications working group, and engages with NATO in preparedness exercises.

1B.4.4 Foreign Investment in U.S. CI/KR

CI/KR protection may be affected by foreign investment and ownership of sector assets. At the Federal level, this issue is monitored by the CFIUS. The committee is chaired by the Secretary of the Treasury, with membership including the Secretaries of State, Defense, Commerce, and Homeland Security; the Attorney General; the Directors of the OMB and the OSTP; the U.S. Trade Representative; the Chairman of the Council of Economic Advisers; the Assistant to the President for Economic Policy; and the Assistant to the President for National Security Affairs.

DHS has important responsibilities regarding various government commissions that support the NIPP. These include:

- As a member of the CFIUS, DHS examines the impact of proposed foreign investments on CI/KR protection. The committee coordinates the development and negotiation of security agreements with foreign entities that may be necessary to manage the risk to CI/KR that a foreign investment may pose. DHS leads government monitoring activities aimed at ensuring compliance with these agreements.
- DHS acts as a partner with DOJ and other executive branch departments in supporting executive branch reviews of applications to the FCC from foreign entities pursuant to section 214 of the Communications Act of 1934 to assess if they pose any threat to CI/KR protection.

1B.4.5 Information Sharing

Effective international cooperation of CI/KR protection requires a system for information sharing that includes processes and protocols for updates among all partners, mechanisms for systematic sharing of best practices, and frequent opportunities for partners to meet to discuss and address international CI/KR issues.

The NOC serves as the Nation's hub for information sharing and situational awareness for domestic incident management and is responsible for increasing coordination (through the NICC) among those members of the international community who are involved because of the role they play in enabling the protection of U.S. CI/KR.

The HSIN supports ongoing information-sharing efforts by offering COIs for selected international partners requiring close coordination with the NOC.

DHS also provides mechanisms, such as the US-CERT portal, to improve information sharing and coordination among government communities and selected international security partners for cyber security. Additionally, the Cybercop portal is a secure Internet-based information-sharing mechanism for law enforcement members involved in the field of electronic crimes investigation. This secure, Internet-based collaborative tool links and supports the law enforcement and investigative community worldwide, serving participants from more than 40 countries.

1B.5 Integration With Other Plans

The NIPP brings a new focus to international security cooperation and provides a risk-based strategic framework for measuring the effectiveness of international activities. The NIPP processes serve as management tools to assess international vulnerabilities and interdependencies. The NIPP process complements long-standing cooperative agreements with Canada, Mexico, the United Kingdom, NATO, and others, and provides the framework for collaborative engagement with additional international partners.

SSPs will include descriptions of sector relationships and security partner roles and responsibilities that address international/multinational organizations and foreign governments. SSPs also will provide a comprehensive view of CI/KR, including the dependencies and interdependencies; international links; and cyber systems needed for the sector to function.

1B.6 Ensuring International Cooperation Over the Long Term

The effort to ensure a sustainable approach to addressing the international aspects of CI/KR protection over the long term requires special consideration in the following areas:

- **Awareness:** Awareness of international aspects of CI/KR protection issues helps ensure implementation of effective, coordinated, and integrated CI/KR protection measures and enables CI/KR security partners to make informed decisions. Often these issues are not apparent to those who can take the most effective action because of the complexity of the international systems affecting CI/KR protection. Awareness programs designed to identify such issues and provide the common framework that allows these issues to be effectively addressed by security partners are required for continued support for protection programs over the long term.
- **Training and Education:** NIPP training topics for the managers and staff responsible for CI/KR that require emphasis include international considerations for CI/KR protection because of the complex considerations that often accompany international linkages and initiatives. Because training and education programs can result in a higher quality workforce for international security partners, they provide benefits over entire careers rather than on a one-time basis as direct aid to international partners often does. Additionally, DHS will ensure that the organizational and sector expertise needed to implement the international aspects of the NIPP program over the long term is developed and maintained through exercises that include adequate testing of international CI/KR protection measures and plans.
- **Research and Development:** Cooperative and coordinated research efforts are one of the most effective ways to improve protective capabilities or to dramatically lower the costs of existing capabilities so that international security partners can afford to do more with their limited budgets. Techniques and designs developed through research can cost very little to share with international security partners and, although the lead times needed for maturation of technology from the laboratory to the field can be decades, such improvements can have wider applicability or much greater effectiveness than available through current methods.
- **Plan Update:** NIPP and SSP updates must reflect the current international situation and must be coordinated, as required, with international agreements affecting CI/KR protection.

Appendix 2: Authorities, Roles, and Responsibilities

Appendix 2A: Summary of Relevant Statutes, Strategies, and Directives

This summary provides additional information on a variety of statutes, strategies, and directives referenced in chapters 2 and 5, as applicable to CI/KR protection. This list is not inclusive of all authorities related to CI/KR protection; rather, it includes the authorities most relevant to national-level, cross-sector CI/KR protection. Please note that there are many other authorities that are related to specific sectors that are not discussed in this appendix; these are left for further elaboration in the SSPs.

2A.1 Statutes

Homeland Security Act of 2002[22]

This act establishes a Cabinet-level department headed by a Secretary of Homeland Security with the mandate and legal authority to protect the American people from the continuing threat of terrorism. In the act, Congress assigns DHS the primary missions to:

- Prevent terrorist attacks within the United States;
- Reduce the vulnerability of the United States to terrorism at home;
- Minimize the damage and assist in the recovery from terrorist attacks that occur; and
- Ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland.

This statutory authority defines the protection of CI/KR as one of the primary missions of the department. Among other actions, the act specifically requires DHS:

[22] Public Law 107-296, November 25, 2002, 116 Stat. 2135. It is codified at 6 U.S.C.

- To carry out comprehensive assessments of the vulnerabilities of the CI/KR of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks;
- To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems; information technology and telecommunications systems (including satellites); electronic financial and property record storage and transmission systems; emergency preparedness communications systems; and the physical and technological assets that support such systems; and
- To recommend measures necessary to protect the CI/KR of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

Those requirements, combined with the President's direction in HSPD-7, mandate the unified approach to CI/KR protection taken in the NIPP.

Critical Infrastructure Information Act of 2002[23]

Enacted as part of the Homeland Security Act, this act creates a framework that enables members of the private sector and others to voluntarily submit sensitive information regarding the Nation's CI/KR to DHS with the assurance that the information, if it satisfies certain requirements, will be protected from public disclosure.

The PCII Program, created under the authority of the act, is central to the information-sharing and protection strategy of the NIPP. By protecting sensitive information submitted through the program, the private sector is assured that the information will remain secure and only be used to further CI/KR protection efforts.[24]

Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act)[25]

The Stafford Act provides comprehensive authority for response to emergencies and major disasters—natural disasters, accidents, and intentionally perpetrated events. It provides specific authority for the Federal Government to provide assistance to State and local entities for disaster preparedness and mitigation, and major disaster and emergency assistance. Major disaster and emergency assistance includes such resources and services as:

- The provision of Federal resources, in general;
- Medicine, food, and other consumables;
- Work and services to save lives and restore property, including:
  - Debris removal;
  - Search and rescue; emergency medical care; emergency mass care; emergency shelter; and provision of food, water, medicine, and other essential needs, including movement of supplies or persons;
  - Clearance of roads and construction of temporary bridges;
  - Provision of temporary facilities for schools and other essential community services;
  - Demolition of unsafe structures that endanger the public;
  - Warning of further risks and hazards;
  - Dissemination of public information and assistance regarding health and safety measures;

[23] The CII Act is presented as subtitle B of title II of the Homeland Security Act (sections 211-215) and is codified at 6 U.S.C. 131 et seq.
[24] Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 8079 (Feb. 20, 2004), are codified at 6 CFR Part 29.
[25] Public Law 93-288, as amended, codified at 42 U.S.C. 68.

  - Provision of technical advice to State and local governments on disaster management and control; and
  - Reduction of immediate threats to life, property, and public health and safety;
- Hazard mitigation;
- Repair, replacement, and restoration of certain damaged facilities; and
- Emergency communications, emergency transportation, and fire management assistance.

Disaster Mitigation Act of 2000

This act amends the Stafford Act by repealing the previous mitigation planning provisions (section 409) and replacing them with a new set of requirements (section 322). This new section emphasizes the need for State, Tribal, and local entities to closely coordinate mitigation planning and implementation efforts.

Section 322 continues the requirement for a State mitigation plan as a condition of disaster assistance, adding incentives for increased coordination and integration of mitigation activities at the State level through the establishment of requirements for two different levels of State plans—standard and enhanced. States that demonstrate an increased commitment to comprehensive mitigation planning and implementation through the development of an approved Enhanced State Plan can increase the amount of funding available through the Hazard Mitigation Grant Program (HMGP). Section 322 also established a new requirement for local mitigation plans and authorized up to 7 percent of HMGP funds available to a State to be used for development of State, local, and tribal mitigation plans.

Corporate and Criminal Fraud Accountability Act of 2002 (also known as the Sarbanes-Oxley Act)[26]

The act applies to entities required to file periodic reports with the Securities and Exchange Commission under the provisions of the Securities and Exchange Act of 1934, as amended. It contains significant changes to the responsibilities of directors and officers, as well as the reporting and corporate governance obligations of affected companies. Among other things, the act requires certification by the company's CEO and chief financial officer that accompanies each periodic report filed that the report fully complies with the requirements of the securities laws and that the information in the report fairly presents, in all material respects, the financial condition and results of the operations of the company. It also requires certifications regarding internal controls and material misstatements or omissions, and the disclosure on a "rapid and current basis" of information regarding material changes in the financial condition or operations of a public company. The act contains a number of additional provisions dealing with insider accountability and disclosure obligations, and auditor independence. It also provides severe criminal and civil penalties for violations of the act's provisions.

The Defense Production Act of 1950 and the Defense Production Reauthorization Act of 2003

This act provides the primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response. Among other powers, this act authorizes the President to demand that companies accept and give priority to government contracts that the President "deems necessary or appropriate to promote the national defense," and allocate materials, services, and facilities, as necessary, to promote the national defense in a major national emergency. This act also authorizes loan guarantees, direct loans, direct purchases, and purchase guarantees for those goods necessary for national defense. It also allows the President to void international mergers that would adversely affect national security. This act defines "national defense" to include critical infrastructure protection and restoration, as well as activities authorized by the emergency preparedness sections of the Stafford Act. Consequently, the authorities stemming from the Defense Production Act are available for activities and measures undertaken in preparation for, during, or following a natural disaster or accidental or malicious event. Under the act and related Presidential orders, the Secretary of Homeland Security has the authority to place and, upon application, authorize State and local governments to place priority-rated contracts in support of Federal, State, and local emergency preparedness activities. The Defense Production Act has a national security nexus with the NIPP. National emergencies related to CI/KR may arise that require the President to use his authority under the Defense Production Act.

[26] Public Law 107-204, July 30, 2002.

The Freedom of Information Act[27]

This act generally provides that any person has a right, enforceable in court, to obtain access to Federal agency records, except to the extent that such records are protected from public disclosure by nine listed exemptions or under three law enforcement exclusions. Persons who make requests are not required to identify themselves or explain the purpose of the request. The underlying principle of FOIA is that the workings of government are for and by the people and that the benefits of government information should be made broadly available. All Federal Government agencies must adhere to the provisions of FOIA with certain exceptions for work in progress, enforcement confidential information, classified documents, and national security information. FOIA was amended by the Electronic Freedom of Information Act Amendment of 1996.

Information Technology Management Reform Act of 1996[28]

Under section 5131 of the Information Technology Management Reform Act of 1996, NIST develops standards, guidelines, and associated methods and techniques for Federal computer systems. Federal Information Processing Standards are developed by NIST only when there are no existing voluntary standards to address the Federal requirements for the interoperability of different systems, the portability of data and software, and computer security.

Gramm-Leach-Bliley Act of 1999[29]

Among other things, this act (title V) provides limited privacy protections on the disclosure by a financial institution of nonpublic personal information. The act also codifies protections against the practice of obtaining personal information through false pretenses.

Public Health Security and Bioterrorism Preparedness and Response Act of 2002[30]

This act improves the ability of the United States to prevent, prepare for, and respond to bioterrorism and other public health emergencies. Key provisions of the act, 42 U.S.C. 247d and 300hh among others, address: (1) development of a national preparedness plan by HHS that is designed to provide effective assistance to State and local governments in the event of bioterrorism or other public health emergencies; (2) operation of the National Disaster Medical System to mobilize and address public health emergencies; (3) grant programs for the education and training of public health professionals and the improvement of State, local, and hospital preparedness for and response to bioterrorism and other public health emergencies; (4) streamlining and clarification of communicable disease quarantine provisions; (5) enhancement of controls on dangerous biological agents and toxins; and (6) protection of the safety and security of food and drug supplies.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)[31]

This act outlines the domestic policy related to deterring and punishing terrorists, and the U.S. policy for CI/KR protection. It also provides for the establishment of a national competence for CI/KR protection. The act establishes the NISAC and outlines the Federal Government's commitment to understanding and protecting the interdependencies among critical infrastructure.

The Privacy Act of 1974[32]

This act provides strict limits on the maintenance and disclosure by any Federal agency of information on individuals that is maintained, including "education, financial transactions, medical history, and criminal or employment history and that contains [the] name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." Although there are specific categories for permissible maintenance of records and limited exceptions to the prohibition on disclosure for legitimate law enforcement and other specified purposes, the

[27] Codified as 5 U.S.C. 552.
[28] Public Law 104-106.
[29] Public Law 106-102 (1999), codified at 15 U.S.C. 94.
[30] Public Law 107-188.
[31] Public Law 107-56, October 26, 2001.
[32] Codified at 5 U.S.C. 552a.

act requires strict recordkeeping on any disclosure. The act also specifically provides for access by individuals to their own records and for requesting corrections thereto.

Federal Information Security Management Act of 2002[33]

This act requires that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets. This legislation is relevant to the part of the NIPP that governs the protection of Federal assets and the implementation of cyber-protective measures under the Government Facilities SSP.

Cyber Security Research and Development Act of 2002[34]

This act allocates funding to NIST and the National Science Foundation for the purpose of facilitating increased R&D for computer network security and supporting research fellowships and training. The act establishes a means of enhancing basic R&D related to improving the cyber security of CI/KR.

Maritime Transportation Security Act of 2002[35]

This act directs initial and continuing assessments of maritime facilities and vessels that may be involved in a transportation security incident. It requires DHS to prepare a National Maritime Transportation Security Plan for deterring and responding to a transportation security incident and to prepare incident response plans for facilities and vessels that will ensure effective coordination with Federal, State, and local authorities. It also requires, among other actions, the establishment of transportation security and crewmember identification cards and processes; maritime safety and security teams; port security grants; and enhancements to maritime intelligence and matters dealing with foreign ports and international cooperation.

Intelligence Reform and Terrorism Prevention Act of 2004[36]

This act provides sweeping changes to the U.S. Intelligence Community structure and processes, and creates new systems specially designed to combat terrorism. Among other actions, the act:

- Establishes a Director of National Intelligence with specific budget, oversight, and programmatic authority over the Intelligence Community;
- Establishes the National Intelligence Council and redefines "national intelligence";
- Requires the establishment of a secure ISE and an information-sharing council;
- Establishes a National Counterterrorism Center, a National Counter Proliferation Center, National Intelligence Centers, and a Joint Intelligence Community Council;
- Establishes, within the Executive Office of the President, a Privacy and Civil Liberties Oversight Board;
- Requires the Director of the FBI to continue efforts to improve the intelligence capabilities of the FBI and to develop and maintain, within the FBI, a national intelligence workforce;
- Directs improvements in security clearances and clearance processes;
- Requires DHS to develop and implement a National Strategy for Transportation Security and transportation modal security plans; enhance identification and credentialing of transportation workers and law enforcement officers; conduct R&D into mass identification technology, including biometrics; enhance passenger screening and terrorist watch lists; improve measures for detecting weapons and explosives; improve security related to the air transportation of cargo; and implement other aviation security measures;

[33] Public Law 107-347, December 17, 2002.
[34] Public Law 107-305, November 27, 2002.
[35] Public Law 107-295, codified at 46 U.S.C. 701.
[36] Public Law 108-458.

- Directs enhancements to maritime security;
- Directs enhancements in border security and immigration matters;
- Enhances law enforcement authority and capabilities, and expands certain diplomatic, foreign aid, and military authorities and capabilities for combating terrorism;
- Requires expanded machine-readable visas with biometric data; implementation of a biometric entry and exit system, and a registered traveler program; and implementation of biometric or other secure passports;
- Requires standards for birth certificates and driver's licenses or personal identification cards issued by States for use by Federal agencies for identification purposes, and enhanced regulations for social security cards;
- Requires DHS to improve preparedness nationally, especially measures to enhance interoperable communications, and to report on vulnerability and risk assessments of the Nation's CI/KR; and
- Directs measures to improve assistance to and coordination with State, local, and private sector entities.

2A.2 National Strategies

The National Strategy for Homeland Security (July 2002)

This strategy establishes the Nation's strategic homeland security objectives and outlines the six critical mission areas necessary to achieve those objectives. The strategy also provides a framework to align the resources of the Federal budget directly to the task of securing the homeland. The strategy specifies eight major initiatives to protect the Nation's CI/KR, one of which specifically calls for the development of the NIPP.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003)

This strategy identifies the policy, goals, objectives, and principles for actions needed to "secure the infrastructures and assets vital to national security, governance, public health and safety, economy, and public confidence." The strategy provides a unifying organizational structure for CI/KR protection and identifies specific initiatives related to the NIPP to drive near-term national protection priorities and inform the resource allocation process.

National Strategy to Secure Cyberspace (February 2003)

This strategy sets forth objectives and specific actions to prevent cyber attacks against America's CI/KR, reduce nationally identified vulnerabilities to cyber attacks, and minimize damage and recovery time from cyber attacks. The strategy provides the vision for cyber security and serves as the foundation for the cyber security component of CI/KR.

The National Strategy for Maritime Security (September 2005)

This strategy provides the framework to integrate and synchronize the existing department-level strategies and ensure their effective and efficient implementation, and aligns all Federal Government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities.

The National Strategy to Combat Weapons of Mass Destruction (December 2002)

This strategy provides policy guidance on combating WMD through three pillars:

- Counter proliferation to combat WMD use;
- Strengthened nonproliferation to combat WMD proliferation; and
- Consequence management to respond to WMD use.

The National Strategy for Combating Terrorism (February 2003)

This strategy provides a comprehensive overview of the terrorist threat and sets specific goals and objectives to combat this threat, including measures to:

- Defeat terrorists and their organizations;
- Deny sponsorship, support, and sanctuary to terrorists;
- Diminish the underlying conditions that terrorists seek to exploit; and
- Defend U.S. citizens and interests at home and abroad.

The National Intelligence Strategy of the United States of America

The National Intelligence Strategy of the United States of America outlines the fundamental values, priorities, and orientation of the Intelligence Community. As directed by the Director of National Intelligence, the strategy outlines the specific mission objectives that relate to efforts to predict, penetrate, and pre-empt threats to national security. To accomplish this, the efforts of the different enterprises of the Intelligence Community are integrated through policy, doctrine, and technology, and by ensuring that intelligence efforts are appropriately coordinated with the Nation's homeland security mission.

2A.3 Homeland Security Presidential Directives

HSPD-1: Organization and Operation of the Homeland Security Council (October 2001)

HSPD-1 establishes the Homeland Security Council and a committee structure for developing, coordinating, and vetting homeland security policy among executive departments and agencies. The directive provides a mandate for the Homeland Security Council to ensure the coordination of all homeland security-related activities among executive departments and agencies and promotes the effective development and implementation of all homeland security policies. The Homeland Security Council is responsible for arbitrating and coordinating any policy issues that may arise among the different departments and agencies under the NIPP.

HSPD-2: Combating Terrorism Through Immigration Policies (October 2001)

HSPD-2 establishes policies and programs to enhance the Federal Government's capabilities for preventing aliens who engage in or support terrorist activities from entering the country, and for detaining, prosecuting, or deporting any such aliens who are in the United States.

HSPD-2 also directs the Attorney General to create the Foreign Terrorist Tracking Task Force to ensure that, to the maximum extent permitted by law, Federal agencies coordinate programs to accomplish the following: (1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and (2) locate, detain, prosecute, or deport any such aliens already present in the United States.

HSPD-3: Homeland Security Advisory System (March 2002)

HSPD-3 mandates the creation of an alert system for disseminating information regarding the risk of terrorist acts to Federal, State, and local authorities, and the public. It also includes the requirement for a corresponding set of protective measures for Federal, State, and local governments to be implemented, depending on the threat condition. Such a system provides warnings in the form of a set of graduated threat conditions that are elevated as the risk of the threat increases. For each threat condition, Federal departments and agencies are required to implement a corresponding set of protective measures.

HSPD-4: National Strategy to Combat Weapons of Mass Destruction (December 2002)

This directive outlines a strategy that includes three principal pillars: (1) Counter-Proliferation to Combat WMD Use, (2) Strengthened Nonproliferation to Combat WMD Proliferation, and (3) Consequence Management to Respond to WMD

Use. It also outlines four cross-cutting functions to be pursued on a priority basis: (1) intelligence collection and analysis on WMD, delivery systems, and related technologies; (2) R&D to improve our ability to address evolving threats; (3) bilateral and multilateral cooperation; and (4) targeted strategies against hostile nations and terrorists.

HSPD-5: Management of Domestic Incidents (February 2003)

HSPD-5 establishes a national approach to domestic incident management that ensures effective coordination among all levels of government, and between the government and the private sector. Central to this approach is the NIMS, an organizational framework for all levels of government, and the NRP, an operational framework for national incident response.

In this directive, the President designates the Secretary of Homeland Security as the principal Federal official for domestic incident management and empowers the Secretary to coordinate Federal resources used for prevention, preparedness, response, and recovery related to terrorist attacks, major disasters, or other emergencies. The directive assigns specific responsibilities to the Attorney General, Secretary of Defense, Secretary of State, and the Assistants to the President for Homeland Security and National Security Affairs, and directs the heads of all Federal departments and agencies to provide their "full and prompt cooperation, resources, and support," as appropriate and consistent with their own responsibilities for protecting national security, to the Secretary of Homeland Security, Attorney General, Secretary of Defense, and Secretary of State in the exercise of leadership responsibilities and missions assigned in HSPD-5.

HSPD-6: Integration and Use of Screening Information (September 2003)

HSPD-6 consolidates the Federal Government's approach to terrorist screening by establishing a Terrorist Screening Center. Federal departments and agencies are directed to provide terrorist information to the Terrorist Threat Integration Center, which is then required to provide all relevant information and intelligence to the Terrorist Screening Center. In order to protect against terrorism, this directive established the national policy to: (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information, as appropriate and to the full extent permitted by law, to support (a) Federal, State, Territorial, local, tribal, foreign government, and private sector screening processes; and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection (December 2003)

HSPD-7 establishes a framework for Federal departments and agencies to identify, prioritize, and protect CI/KR from terrorist attacks, with an emphasis on protecting against catastrophic health effects and mass casualties. This directive establishes a national policy for Federal departments and agencies to identify and prioritize U.S. CI/KR and to protect them from terrorist attacks. HSPD-7 mandates the creation and implementation of the NIPP and sets forth roles and responsibilities for DHS; SSAs; other Federal departments and agencies; and State, local, tribal, private sector, and other security partners.

HSPD-8: National Preparedness (December 2003)

HSPD-8 establishes policies to strengthen the preparedness of the United States to prevent, protect, respond to, and recover from threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal; establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments; and outlining actions to strengthen the preparedness capabilities of Federal, State, and local entities. This directive mandates the development of the goal to guide emergency preparedness training, planning, equipment, and exercises, and to ensure that all entities involved adhere to the same standards. The directive calls for an inventory of Federal response capabilities and refines the process by which preparedness grants are administered, disbursed, and utilized at the State and local levels.

HSPD-9: Defense of United States Agriculture and Food (January 2004)

HSPD-9 establishes an integrated national policy for improving intelligence operations, emergency response capabilities, information-sharing mechanisms, mitigation strategies, and sector vulnerability assessments to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

HSPD-11: Comprehensive Terrorist-Related Screening Procedures (August 2004)

HSPD-11 requires the creation of a strategy and implementation plan for a coordinated and comprehensive approach to terrorist screening in order to improve and expand procedures to screen people, cargo, conveyances, and other entities and objects that pose a threat.

HSPD-12: Policy for a Common Identification for Federal Employees and Contractors (August 2004)

HSPD-12 establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors in order to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. The resulting mandatory standard was issued by NIST as the Federal Information Processing Standard Publication.

HSPD-13: Maritime Security Policy (December 2004)

HSPD-13 directs the coordination of U.S. Government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving the appropriate Federal, State, local, and private sector entities. The directive also establishes a Maritime Security Policy Coordinating Committee to coordinate interagency maritime security policy efforts.

HSPD-14: Domestic Nuclear Detection (April 2005)

HSPD-14 establishes the effective integration of nuclear and radiological detection capabilities across Federal, State, local, and tribal governments and the private sector for a managed, coordinated response. This directive supports and enhances the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as providing appropriate information to these entities.

2A.4 Other Authorities

Executive Order 13231, Critical Infrastructure Protection in the Information Age (October 2001) (amended by E.O. 13286, February 28, 2003)

This Executive order provides specific policy direction to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. It recognizes the important role that networked information systems (critical information infrastructure) play in supporting all aspects of our civil society and economy and the increasing degree to which other critical infrastructure sectors have become dependent upon such systems. It formally establishes as U.S. policy the need to protect against disruption of the operation of these systems and to ensure that any disruptions that do occur are infrequent, of minimal duration, manageable, and cause the least damage possible. The Executive order specifically calls for the implementation of the policy to include "a voluntary public-private partnership, involving corporate and nongovernmental organizations." The Executive order also reaffirms existing authorities and responsibilities assigned to various executive branch agencies and interagency committees to ensure the security and integrity of Federal information systems generally and of national security information systems in particular.

National Infrastructure Advisory Council

In addition to the foregoing, Executive Order 13231 (as amended by E.O. 13286 of February 28, 2003, and E.O. 13385 of September 29, 2005) also established the NIAC as the President's principal advisory panel on critical infrastructure protection issues spanning all sectors. The NIAC is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and State and local government, representing senior executive leadership expertise from the critical infrastructure and key resource areas as delineated in HSPD-7.

The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructure, both physical and cyber, supporting important sectors of the economy. It also has the authority to provide advice directly

to the heads of other departments that have shared responsibility for critical infrastructure protection, including HHS, DOT, and DOE. The NIAC is charged to improve the cooperation and partnership between the public and private sectors in securing critical infrastructure and advises on policies and strategies that range from risk assessment and management, to information sharing, to protective strategies and clarification on roles and responsibilities between public and private sectors.

Executive Order 12382, President's National Security Telecommunications Advisory Committee (amended by E.O. 13286, February 28, 2003)

This Executive order creates the NSTAC, which provides to the President, through the Secretary of Homeland Security, information and advice from the perspective of the telecommunications industry with respect to the implementation of the National Security Telecommunications Policy.

Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions (amended by E.O. 13286, February 28, 2003)

Executive Order 12472 assigns NS/EP telecommunications functions, including wartime and non-wartime emergency functions, to the National Security Council, OSTP, Homeland Security Council, OMB, and other Federal agencies. The Executive order seeks to ensure that the Federal Government has telecommunications services that will function under all conditions, including emergency situations. This Executive order establishes the NCS with the mission to assist the President, the National Security Council, the Homeland Security Council, the Director of OSTP, and the Director of the OMB in: (1) the exercise of telecommunications functions and responsibilities set forth in the Executive Order; and (2) the coordination of planning for and provision of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.

Appendix 2B: NIPP Initial Implementation Initiatives and Actions

This appendix specifies the initiatives, actions, and milestones that are necessary for NIPP implementation. The matrix below defines the shared responsibilities for NIPP implementation and identifies security partners with primary and supporting responsibility for each of the initiatives and actions specified. Milestones are specified in terms of the number of days after NIPP final approval, or by a specific date. Actions are organized by NIPP chapter to provide a ready reference to the more detailed information that is provided in the NIPP Base Plan.

Notes: **x** = Primary responsibility **o** = Support responsibility (may be required to qualify for grants)
+ = Milestone indicator NLT = Not later than

Chapter	Implementation Actions	Milestone				Security Partner					
		NLT 90 Days After NIPP Approval	NLT 180 Days	NLT 365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal Agency	State or Territory	Local and Tribal	Private Sector
2	**AUTHORITIES, ROLES, AND RESPONSIBILITIES**										
	Review NIPP and establish processes needed to support NIPP implementation.	+				x	x	x	x	x	x
	Incorporate NIPP into strategies for cooperation with foreign countries and international/multinational organizations.		+			x	x	x	o	o	o
3	**THE PROTECTION PROGRAM STRATEGY: MANAGING RISK**										
	Develop sector-specific CI/KR inventory guidance.		+			x	x	o	o	o	o
	Review existing risk assessment methodologies to determine compatibility with the NIPP baseline criteria.		+			x	x	x	x	x	x
	Establish timeline for: (1) the development of sector-specific risk methodologies, and (2) for conducting consequence-based top-screening for all CI/KR sectors.		+			x	x	o	o	o	o
	Conduct and validate consequence assessments of priority CI/KR as identified by the top-screening process.			+		x	x	x	x	x	x
	Conduct or facilitate vulnerability assessments in priority CI/KR sectors and identify cross-sector vulnerabilities.			+		x	x	x	x	x	x
	Develop sector-specific CI/KR threat assessments needed to support comprehensive risk assessments.	+				x	o	o	o	o	o
	Provide guidance on metrics for annual reporting and national-level, cross-sector comparative analysis.	+				x	o	o	o	o	o
4	**ORGANIZING AND PARTNERING FOR CI/KR PROTECTION**										
	Establish all SCCs, GCCs, and SLTGCC in accordance with the NIPP partnership model.	+				x	x	o	o	o	o
	Complete rollout of HSIN-CS COI; implement policies for vetting and disseminating information to security partners.			+		x	x	o	o	o	o
	Identify sector-level information-sharing mechanisms and ensure that information protection practices comply with appropriate guidance for protection of classified or sensitive information. Publish PCII final rule.	+				x	x	o	o	o	o
	Develop Annual CI/KR Protection Information Requirements Report.		+			x	o	o	o	o	o
	Work with the Department of State to review the charter and coordinating mechanisms for the interagency working group that coordinates U.S. international CI/KR protection outreach and update as needed to align with the NIPP.	+				x	x	x	o	o	o

Chapter	Implementation Actions	Milestone				Security Partner					
		NLT 90 Days After NIPP Approval	NLT 180 Days	NLT 365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal Agency	State or Territory	Local and Tribal	Private Sector
5	**INTEGRATING CI/KR PROTECTION AS PART OF THE HOMELAND SECURITY MISSION**										
	Coordinate SSP development in collaboration with security partners and submit to DHS with appropriate documentation of concurrence.		+			o	x	o	o	o	o
	Review and revise CI/KR-related plans as needed to reinforce linkage between NIPP steady-state CI/KR protection and NRP incident management requirements.		+			x	x	x	x	x	x
	Review current CI/KR protection measures to ensure alignment with HSAS threat conditions and specific threat vectors/scenarios.		+			x	x	x	x	x	x
6	**ENSURING AN EFFECTIVE, EFFICIENT PROGRAM OVER THE LONG TERM**										
	Develop and implement a comprehensive national CI/KR protection awareness program.		+			x	x	o	o	o	o
	Review and, as appropriate, revise training programs to ensure consistency with NIPP requirements.		+			x	x	x	x	x	x
	Provide initial NIPP training to security partners.	+				x	x	o	o	o	o
	Ensure that national exercises include CI/KR protection and interaction between the NIPP and the NRP.	+				x	x	o	o	o	o
	Communicate requirements for CI/KR-related R&D to DHS for use in the national R&D planning effort.				July 1 (Annually)	o	x	x	o	o	o
	Identify all databases, data services and sources, and modeling capabilities with CI/KR application.		+			x	x	x	x	x	x
	Conduct first annual review of the NIPP and SSPs.			+		x	x	x	x	x	x
7	**PROVIDING RESOURCES FOR THE CI/KR PROTECTION PROGRAM**										
	Submit Sector CI/KR Protection Annual Report to DHS				July 1 (Annually)	o	x	o	o	o	o
	Submit National CI/KR Protection Annual Report to the Executive Office of the President.				Sep 1 (Annually)	x	o	o	o	o	o
	Review homeland security grant guidance to ensure that requirements are consistent with the NIPP.	+				x	o	o	o	o	o
	Advise State, local, and tribal governments of SSA grant programs and/or other sources that can support the NIPP.		+			x	x	o	o	o	o
	Apply for homeland security grants to address CI/KR protection efforts per DHS/G&T guidance.				*	o	o	o	x	x	o

* Required application deadlines are specified within individual program guidance and may change annually. Dates for submitting grant applications, program requirements, and other required reports to DHS will be specified in annual grant program guidance and application kits. States will work with local and tribal jurisdictions to ensure compliance with all other related reporting requirements.

Appendix 3: The Protection Program

Appendix 3A: NIPP Baseline Criteria for Assessment Methodologies

The purpose of this appendix is to specify the baseline criteria for methodologies used to support all levels of comparative risk analysis under the NIPP framework. Many owners and operators have performed vulnerability and/or risk assessments on the assets, systems, and networks under their control. To take advantage of these activities, DHS and the SSAs will use the results from previously performed assessments wherever possible. However, the assessment work to date has varied widely both within and across sectors in terms of its assumptions, comprehensiveness, objectivity, inclusion of threat and consequence considerations, physical and cyber dependencies, and other characteristics. In order to use previous assessment results to support national comparative risk analysis, the methodologies used to perform the assessments must be tested against the NIPP baseline criteria.

3A.1 Baseline Criteria

There are seven criteria that constitute the national baseline, categorized generally into two different groups. The first group tests the methodology to ensure that it will be credible to objective users of the analysis produced by methodology; the second group tests the methodology to ensure that it will be comparable with other standard methods used in comparative sector or national risk assessment.

To be credible, a methodology must have a sound basis (it must have integrity); it also must be complete and the analytic method and associated assumptions must be defensible. These factors are reflected in the first three elements of the criteria. To be comparable, the methodology must be documented, transparent, reproducible, and accurate; these factors are reflected in the last four elements of the criteria.

The following questions provide a simple way to determine which aspects of a methodology meet the baseline criteria. The questions also provide a guide for improving the methodologies or changing them so that they can meet the baseline criteria. A methodology meets the requirements of the baseline criteria when all of the questions can be answered in the affirmative.

Is the Methodology Credible?

1. **Integrity (sound basis):** Is the methodology based on documented risk analysis and security vulnerability analysis? Does it specifically address:

   a. Consequences?
   b. Vulnerability?
   c. Threat?

2. **Complete**: Does the methodology provide reasonably complete results via a quantitative, systematic, and rigorous process that:

   a. Provides numerical values for estimated consequences, vulnerability, and threat whenever possible, or uses scales when numerical values are not practical?
   b. Specifically addresses both public health and safety and direct economic consequences?
   c. Considers existing protective measures and their effects on vulnerabilities as a baseline?
   d. Examines physical, cyber, and human vulnerabilities?
   e. Applies the worst-reasonable-case standard when assessing consequences and choosing threat scenarios?
   f. Uses threat-based vulnerability assessments?

3. **Defensible:** Is the methodology thorough and does it use the recognized methods of the professional disciplines relevant to the analysis? Does it adequately address the relevant concerns of government, the CI/KR workforce, and the public?

Is the Methodology Comparable to Other Methodologies?

1. **Documented:** Does the methodology provide clear and sufficient documentation of the analysis process and the products that result from its use?

2. **Transparent:** Is the methodology easily understandable to others as to:

   a. Assumptions used?
   b. Key definitions?
   c. Units of measurement?
   d. How it is to be accomplished?
   e. Basis for expert judgments and risk decisions?

3. **Reproducible:** Does the methodology provide results that are reproducible or verifiable by equivalently experienced or knowledgeable personnel?

4. **Accurate:** Is the methodology free from significant errors or omissions so that the results are suitable to inform decisionmaking?

Given the unique nature of the individual CI/KR sectors and the assets, systems, and networks that comprise them, details of the baseline criteria must be tailored to each sector. DHS will work with the SSAs and other sector security partners to accomplish this tailoring; however, the baseline criteria above are generally applicable to each sector.

Existing assessments or methodologies will be considered by DHS as meeting the NIPP Baseline Criteria and, therefore, are suitable for national and sector-level comparative risk analysis if they can provide an affirmative response to the questions above. Assessment or methodology evaluations will be done in coordination with the SSA, SCC, and GCC, as appropriate.

3A.2 Specific Aspects of the NIPP Baseline Criteria

Based on classical risk analysis. As outlined in chapter 3 of the NIPP, risk analysis consists of three primary elements: consequence, vulnerability, and threat. To be considered credible, a proposed methodology must include all three components of risk.

Provide numerical values when possible; use scales when necessary. Risk typically can be measured either quantitatively (i.e., numerically) or qualitatively (i.e., descriptively). Public health and safety and economic impacts generally lend themselves to quantitative measurement (e.g., number of lives lost, cost in dollars of rebuilding or restoring an asset), whereas psychological and governance impacts are often measured qualitatively. For quantitatively measured consequences and their associated risk, accurate numerical estimates should be used whenever possible. When it is not practical to use such estimates, scales should be used to reflect the assessed outcome using either numerical ranges (for quantitative metrics) or detailed descriptions (for qualitative metrics). The use of numerical ranges and/or detailed descriptions is necessary because terms such as "low" or "high" are subject to varied interpretation by different users. DHS will provide sample ranges and descriptive language to security partners, and will work with them to establish "translators" that facilitate the conversion of results using other methodologies to standard scales to support national comparative risk analysis.

Consider human and direct economic consequences. For the national comparative risk analysis conducted by DHS, the consequences of interest are those of national significance as established in HSPD-7. These consequences can be divided into four main categories: human, economic, public confidence, and government capability. Because accurately estimating consequences other than direct injury, loss of life, and economic effects is complex and often beyond the scope of an individual owner/operator's expertise, this element of the baseline criteria requires assessment methodologies to address the following two types of impact at a minimum:

- **Human Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries).
- **Economic Impact:** Direct effects on the national, State, tribal, or local economy (e.g., cost to rebuild facility, system, or network; cost to respond to and recover from attack; other clearly definable incident costs resulting from unavailability of product or service; or long-term costs due to environmental damage).

Consider existing protective measures and their impacts as the baseline. In evaluating the extent to which an asset, system, or network is vulnerable or an attack is likely, an assessment should consider the existing measures that are in place to reduce that asset, system, or network's exposure to the relevant threat scenarios. Specifically, security specialists should examine the ability of an asset, system, or network's existing security profile to deter, detect, devalue, defend against, mitigate, respond to, and recover from the most relevant threat scenarios.

Use worst-reasonable-case standard. Risk assessments are significantly influenced by the estimated or assumed level of success or severity of a given threat scenario (e.g., worst case, worst reasonable case, most likely). For the purposes of national comparative risk assessment, methodologies should use a worst-reasonable-case scenario.

Examine physical, cyber, and human vulnerabilities. When evaluating risk, many vulnerability assessments focus solely on physical security; however, physical security is only one aspect of a robust vulnerability assessment. Vulnerability assessments should also assess personnel security and other human security issues, cyber security and network architecture issues, operational security, and infrastructure dependencies and interdependencies.

Scenario-based vulnerability assessments. The suite of tools that DHS is developing and using for vulnerability assessments is scenario based, meaning that the assessments measure the susceptibility of an identified asset, system, or network to a specific threat scenario (e.g., successful detonation of a nuclear bomb, successful detonation of a car bomb, etc.). This allows the assessment to be informed in general terms by potential adversary tactics and attack vectors. Consequently, vulnerability assessment methodologies used to support cross-sector comparative risk analyses should be scenario based, and certain

specific scenarios or their equivalent should be used. In light of the distinct characteristics associated with different types of assets, systems, or networks, DHS will work with sector partners to identify which threat scenarios are most appropriate in the context of the sector-specific landscape.

Defensible on logical grounds. In order to produce analysis that is credible to those who must use its results, a methodology must adhere to the recognized methods of the professional disciplines that are relevant to the method of analysis (e.g., economics, engineering, medical profession), and it must reasonably and adequately address the concerns raised by the three groups who may be directly affected by the decisions based on its results: (1) governments at all levels, (2) the CI/KR workforce, and (3) the public at large.

Documentation is necessary to enable comparison with other methodologies in use. Written documentation that is clear and sufficiently complete to allow a comparison of strengths and weaknesses with respect to other methodologies used in the national comparative risk assessment is necessary. This should include a description of assumptions, definitions, units of measurement, time horizon, the general order and steps of the assessment, calculations, and the basis for any expert judgments that the methodology relies on that are not readily apparent.

Need to be easily understandable. In addition to the existence of written documentation, a methodology must be easily understandable to others with appropriate knowledge and experience. This means that:

- Assumptions must be stated;
- Key definitions must be provided;
- Units of measurement must be specified;
- Analytic process by which the methodology is executed must be specified; and
- Basis for expert judgments used in lieu of explicit calculations or analysis must be provided.

As with any deliberate process, the results of applying the methodology must be reproducible or verifiable by others of requisite knowledge and experience levels. The methodology must be sufficiently defined and deliberate so that any qualified person could replicate the results it produces; it must not depend on hidden judgments or opinions.

Must be free from logical errors of omission or commission. Because the results of risk assessments will be used to inform decisions regarding homeland security, the accuracy of the methodology must meet a high standard. While estimates and approximations often must be used, the tradeoff between practicality and accuracy must be carefully taken into account and, in no case, should logical or mathematical errors be accepted.

Appendix 3B: Existing Protective Programs and Other In-Place Measures

This appendix provides examples of the Federal protective programs that currently support NIPP implementation. The examples provided herein generally cut across sectors and have national significance. These Federal programs augment the extensive State, local, tribal, and private sector protective programs that constitute important efforts already being implemented in support of the NIPP. The SSPs address sector-specific programs that are conducted under the leadership of the SSAs, and include selected protection programs undertaken by other security partners that apply broadly across the sector.

3B.1 Protective Programs and Initiatives

Assistance Visits: This activity refers to facility-level security assessments conducted by a federally led team and facility owners and operators that are designed to facilitate vulnerability identification and mitigation discussions between security partners and individual CI/KR owners and operators.

Buffer Zone Protection Program: The BZPP is a grant program designed to provide resources to State, local, and tribal law enforcement and other security professionals to enhance security of priority CI/KR facilities, thereby making it more difficult for terrorists to conduct surveillance or successfully launch an attack from the immediate vicinity of a potential target.

Comprehensive Reviews: DHS is leading an interagency effort to develop and conduct comprehensive reviews of select potentially high-risk CI/KR. The Comprehensive Review Program spans multiple CI/KR sectors. Working collaboratively with private sector owners and operators, State and local law enforcement and first-responders, and other security partners, a DHS-led interagency team first collects data available from multiple agencies; invites owners and operators to provide additional data; and, if required, visits specific locations to gather additional information that is needed. The team then evaluates the potential

consequences and vulnerabilities of a given asset or group of like assets from high-consequence and/or high-risk sectors within a specific geographical area, as well as the protective and response capabilities associated with the facility and the surrounding community.

Comprehensive reviews will assist State and local jurisdictions in identifying vulnerabilities and capability gaps so they may be addressed in State and local homeland security strategies and CI/KR protection programs.

As the comprehensive review process matures, DHS and the SSAs expect to learn a great deal about the development and execution of joint programs and to employ these lessons in building partnerships, thereby increasing the efficiency of Federal CI/KR protection activities and reinforcing the value of a coordinated approach. Federal agencies with sector-based security responsibilities should plan and budget for participation in the Comprehensive Review Program.

Control Systems Security Initiative: DHS sponsors programs to increase the security of control systems. A control system is an interconnection of components (designed to maintain operation of a process or system) connected or related in such a manner as to command, monitor, direct, or regulate itself or another system. Control systems are embedded throughout the Nation's CI/KR and may be vulnerable to increasing cyber threats that could have a devastating impact on national security, economic security, public health and safety, and the environment. The DHS Control Systems Security Initiative provides coordination among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CI/KR sectors.

Federal Cyber System Security Programs: DHS established the GFIRST to facilitate interagency information sharing and cooperation across Federal agencies responsible for cyber system readiness and response. The members work together to understand and manage computer security incidents and to encourage proactive and preventive security practices. Other examples of Federal agency cyber security access control, certification, and policy enforcement tools include:

- The General Services Administration (GSA) is responsible for developing and implementing an infrastructure for authentication services, as well as an automated risk assessment tool for government-wide use in certifying and accrediting its eAuthentication gateway. GSA is creating a list of approved solution providers that supply smart cards based on Federal Public Key Infrastructure standards and that include a new electronic authentication policy specification.
- The National Oceanic and Atmospheric Agency has implemented enterprise-wide vulnerability assessments and virus-detection software, an intrusion-detection system, anti-virus scanning gateways, and a patch management policy.

Federal Hazard Mitigation Programs: FEMA administers three programs that provide funds for activities that reduce losses from future disasters or help prevent the occurrence of catastrophes. These hazard mitigation programs include the Flood Mitigation Assistance Program, the Hazard Mitigation Grant Program, and the Pre-Disaster Mitigation Program. These programs enable grant recipients to undertake activities such as the elevation of structures in floodplains, relocation of structures from floodplains, construction of structural enhancements to facilities and buildings in earthquake-prone areas (also known as retrofitting), and modifications to land-use plans to ensure that future construction ameliorates, and does not exacerbate, hazardous conditions.

International Outreach Program: DHS works with the Department of State and other security partners to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of best practices, training, and other programs, as needed, to improve the protection of overseas assets and the reliability of the foreign infrastructure on which the United States depends.

Internet Disruption Contingency Planning: DHS formed a strategic partnership through the Internet Disruption Working Group in January 2005 to assist the NCRCG, the US-CERT, and the private sector to coordinate contingency plans for recovering Internet functions in the event of a cyber-related incident. This working group collaborates with major security partners to identify and prioritize the short-term protective measures necessary to prevent major disruptions of the Internet or reduce their consequences and to identify responsive/reconstitution measures for contingency plans in the event of a major disruption.

National Cyber Exercises: DHS conducts exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, Territorial, local, tribal, and international government elements, as well as private sector corporations and coordinating councils.

National Cyber Response Coordination Group: This entity facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences (collectively known as cyber incidents). The NCRCG serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of the Federal Government's response and recovery efforts during a cyber crisis. It uses established relationships with the private sector and State and local governments to help manage a cyber crisis, develop courses of action, and devise appropriate response and recovery strategies.

Protective Community Support Program: Specific advisory support is provided to the protective community (e.g., law enforcement, first-responders), including training and exercise support.

Protective Security Advisor Program: DHS protection specialists are assigned as liaisons between DHS and the protective community at the State, local, and private sector levels in geographical areas representing major concentrations of CI/KR across the United States. The PSAs are responsible for sharing risk information and providing technical assistance to local law enforcement and CI/KR owners and operators of CI/KR within those areas.

Software Assurance: DHS is developing best practices and new technologies to promote integrity, security, and reliability in software development. Focused on shifting away from the current security paradigm of patch management, DHS is leading the Software Assurance Program, a comprehensive strategy that addresses processes, technology, and acquisition throughout the software life cycle to result in secure and reliable software that supports critical mission requirements.

Training Programs: DHS training programs are designed to provide security partners with a source from which they can obtain specialized training to enhance CI/KR protection. Subject matter, course length, and location of training can be tailored to security partner needs.

3B.2 Guidelines, Reports, and Planning

Cyber Security Planning: DHS recognizes that each sector will have a unique reliance on cyber systems and will, therefore, assist SSAs in considering a range of effective and appropriate cyber protective measures. The sector-level approaches to cyber security will be documented in the respective SSPs.

Educational Reports: DHS provides several types of informational reports to support efforts to protect CI/KR. They cover subjects such as CI/KR common vulnerabilities, potential indicators of terrorist activity, and best practices for protective measures. As they are developed, these reports are distributed to all State and Territorial Homeland Security Offices with the guidance that they should be shared with CI/KR owners and operators, the law enforcement community, and captains of the ports in their respective jurisdictions.

Risk Management Manuals: In response to the September 11, 2001, attacks, FEMA's role was expanded to include activities to reduce the vulnerability of buildings to terrorist attacks. In support of this, FEMA created the Risk Management Series, a collection of publications directed at providing design guidance to mitigate the consequences of manmade disasters.

To date, the series includes the following manuals:

- FEMA 155, Building Design for Homeland Security
- FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 427, Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks

- FEMA 428, Primer to Design Safe School Projects in Case of Terrorist Attacks
- FEMA 429, Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings
- FEMA 430, Primer for Incorporating Building Security Components in Architectural Design
- FEMA 452, Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings
- FEMA 453, Multihazard Shelter (Safe Havens) Design

3B.3 Information-Sharing Programs That Support CI/KR Protection

Federal agencies and the law enforcement community provide information-sharing services and programs that support CI/KR protection information sharing. These include:

- **DHS Homeland Security Information Network:** HSIN is a national, Web-based communications platform that allows DHS; SSAs; State, local, and tribal government entities; and other security partners to obtain, analyze, and share information based on a common operating picture of strategic risk and the evolving incident landscape. The network is designed to provide a robust, dynamic information-sharing capability that supports both NIPP-related steady-state CI/KR protection and NRP-related incident management activities, and to provide the information-sharing processes that form the bridge between these two homeland security missions. HSIN will be one part of the ISE called for by the Intelligence Reform and Terrorism Prevention Act of 2004; as specified in the act, it will provide users with access to terrorism information that is matched to their roles, responsibilities, and missions in a timely and responsive manner. HSIN is discussed in detail in chapter 4.
- **FBI's InfraGard:** InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence related to the protection of U.S. CI/KR from both physical and cyber threats. InfraGard chapters are geographically linked with FBI Field Office territories. Each InfraGard chapter has an FBI Special Agent Coordinator who works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters.
- **Interagency Cyber Security Efforts:** Interagency cooperation and information sharing are essential to improving national counterintelligence and law enforcement capabilities pertaining to cyber security. The intelligence and law enforcement communities have various official and unofficial information-sharing mechanisms in place. Examples include:
  - **U.S. Secret Service's Electronic Crimes Task Forces:** U.S. Secret Service's ECTFs provide interagency coordination on cyber-based attacks and intrusions. At present, 15 ECTFs are in operation, with an expansion planned.
  - **FBI's Inter-Agency Coordination Cell:** The Inter-Agency Coordination Cell is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
  - **Computer Crime and Intellectual Property Section:** DOJ, Criminal Division, Computer Crime and Intellectual Property Section is responsible for prosecuting nationally significant cases of cyber crime and intellectual property crime. In addition to its direct litigation responsibilities, the division formulates and implements criminal enforcement policy and provides advice and assistance.
  - **Cybercop Portal:** The DHS-sponsored Cybercop portal is a secure Internet-based information-sharing mechanism that connects more than 5,300 members of the law enforcement community worldwide (including bank investigators and the network security community) involved in electronic crimes investigations.

- **Law Enforcement Online:** The FBI provides LEO as national focal point for electronic communications, education, and information sharing for the law enforcement community. LEO, which can be accessed by any approved employee of a Federal, State, or local law enforcement agency, or approved member of an authorized law enforcement special interest group, is intended to provide a communications mechanism to link all levels of law enforcement throughout the United States.
- **Regional Information Sharing Systems:** The RISS Program is a federally funded program administered by DOJ, Office of Justice Programs, Bureau of Justice Assistance. RISS serves more than 7,300 member law enforcement agencies in 50 States, the District of Columbia, Guam, Puerto Rico, the U.S. Virgin Islands, Australia, Canada, and the United Kingdom. The program is comprised of six regional centers that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are terrorism, drug trafficking, violent crime, cyber crime, gang activity, and organized criminal activities. The majority of the member agencies are at the municipal and county levels; however, more than 485 State agencies and more than 920 Federal agencies also participate. The Drug Enforcement Administration; FBI; U.S. Attorneys' Offices; Internal Revenue Service; Secret Service; U.S. Immigration and Customs Enforcement; and the Bureau of Alcohol, Tobacco, Firearms, and Explosives are among the Federal agencies participating in the RISS Program.
- **Sharing National Security Information:** The ability to share relevant classified information poses a number of challenges, particularly when the majority of industry facilities are neither designed for nor accredited to receive, store, and dispose of these materials. Ultimately, HSIN may be used to more efficiently share appropriate classified national security information with cleared private sector owners and operators during incidents, times of heightened threat, or on an as-needed basis. While supporting technologies and policies are identified to satisfy this requirement, DHS will continue to expand its initiative to sponsor security clearances for designated private sector owners and operators, sharing classified information using currently available methods.
- **Web-Based Services for Citizens:** A variety of Web-based information services are available to enhance the general awareness and preparedness of American citizens. These include CitizenCorps.gov, FirstGov.gov, Ready.gov, and USAonwatch.org.

Appendix 3C: National Asset Database

3C.1 Why Do We Need a National CI/KR Inventory?

HSPD-7 directs the Secretary of Homeland Security to lead efforts to reduce the Nation's vulnerability to terrorism and deny the use of infrastructure as a weapon by developing, coordinating, integrating, and implementing plans and programs that identify, catalog, prioritize, and protect CI/KR in cooperation with all levels of government and private sector entities. A central Federal data repository for analysis and integration is required to provide DHS with the capability to identify, collect, catalog, and maintain a national inventory of information on assets, systems, networks, and functions that may be critical to the Nation's well being, economy, and security. This inventory is also essential to help inform decisionmaking and specific response and recovery activities pertaining to natural disasters and other emergencies.

To fulfill this need, DHS has developed the NADB, a continually evolving and comprehensive catalog of the assets, systems, and networks that comprise the Nation's CI/KR. The NADB contains descriptive information regarding CI/KR and is the primary Federal repository for CI/KR information. Although the NADB is not a listing of prioritized assets, it has the capability to be queried in many ways that can help inform risk-mitigation activities across the CI/KR sectors and government jurisdictions.

3C.2 How Does the Inventory Support the NIPP?

The NADB provides a coordinated and consistent framework to incorporate and display the CI/KR data submitted by Federal, State, and local agencies; the private sector; and integrated Federal or commercial databases. The framework and structure of the NADB have been constructed to readily integrate and provide the required data in a usable and effective manner. Two primary components of this framework are the categorization structure and the infrastructure type data fields:

- The **categorization structure** groups CI/KR by sector and identifies overlaps between and across sectors. It was developed in coordination with the SSAs to ensure that every CI/KR type is represented.

- The **infrastructure type data fields** outline the attributes of interest that are integral to assessment and analysis per a specific category of CI/KR. The information contained in these data fields feeds the strategic risk assessment process used to prioritize CI/KR in the context of terrorist threats or incidents, natural disasters, or other emergencies.

The information in the NADB enables the analysis necessary to determine which assets, systems, and networks comprise the Nation's CI/KR, and to inform security planning and preparedness, resource investments, and post-incident response and recovery activities within and across sectors and governmental jurisdictions.

3C.3 What Is the Current Content of the Inventory?

- DHS gathers data related to the Nation's CI/KR from a variety of sources. The present inventory reflects a collection of information garnered from formal data calls, voluntary additions, and the leveraging of various Federal and commercial databases. Information for the database is received from Federal agencies, State and local submissions, voluntary private sector submissions, commercial demographics products, external data sources, and subject matter experts. The information is used to inform CI/KR protection efforts, contingency planning, planning for implementation of initiatives such as the BZPP, and to aid decisionmakers during response, recovery, and restoration following terrorist attacks, natural disasters, or other emergencies.

3C.4 How Will the Current Inventory Remain Accurate?

DHS continues to seek input from multiple sources, including existing databases managed by SSAs, commercial providers, State and local governments, and the private sector. Integrating existing databases will provide a dynamic common operating interface of infrastructure and vulnerability information through a cross flow of data between separate databases, or links to provide access to other databases. Existing databases being considered for integration are shown in table 3C-1. Ownership and control of the data will be determined according to the circumstances of each database. Classification of the data will be based on Original Classification Authority (OCA) guidance and will be protected as required by OCA guidance and direction.

Table 3C-1: Database Integration

Database	Use
Infrastructure and Critical Asset Viewer (iCAV)	DHS is leveraging existing geospatial capabilities and technology used by the National Geospatial-Intelligence Agency by implementing the iCAV as a DHS Geospatial Enterprise Solution for geospatial mapping, analysis, and sorting of the Nation's CI/KR. The iCAV system will use the geospatial component to spatially display and map information contained in the NADB.
National Threat Incident Database	This database provides a source of consolidated information concerning credible threats and incidents related to our Nation's CI/KR.
DHS LENS Vulnerability Databases	These databases contain Common Vulnerability and Potential Terrorist Activity Indicator Reports, and site assistance visits and BZPP schedules. Site assistance visits and BZPP documents will be available through classified and unclassified secure portals as applicable.
Commercial/Sector-Specific Databases	Many existing Federal and commercial databases contain information sets pertinent to the NADB. Commercial databases will be purchased based on available funding and priorities for information requirements. An example of one such commercially available database is iMapData, a Web-based geospatial subscription service with access to geo-referenced data sets covering physical infrastructure, emergency services, government facilities, political boundaries, military installations, media distribution areas, educational facilities, business locations, and demographic breakdowns.

3C.5 How Will the Database Be Maintained?

The process of ensuring that the data collected is both current and accurate, and that user requirements are incorporated into the portal as necessary, is continual. Data updates and currency are largely dependent upon the sources of the data and the frequency of the updates that they provide.

Efficiency and reliability have been maintained through the implementation of unique numerical identifiers designed to facilitate the efficient integration of information from multiple databases. Verification and validation efforts by contracted companies or Federal employees will play a key role in ensuring information currency. Eventually, all approved users given access to the NADB will have the ability to provide updated information to the NADB Program Office for review prior to inclusion in the inventory.

Feedback forms are also incorporated to provide user recommendations, changes, requirements, and/or feedback to DHS. User requirements will help drive capabilities and functionality of future evolutions and versions of the inventory.

3C.6 What Are the Security Partner Roles and Responsibilities?

The development and population of the NADB is highly dependent upon the participation and support of the SSAs, the States, and private sector entities:

- SSAs have primary responsibility for providing sector information to DHS for inclusion in the NADB using the format and categorization system employed by the NADB.[37] The processes used for sector CI/KR and database identification in coordination with security partners will be described in the SSPs.
- Some State governments have either already developed infrastructure databases or have begun the process to identify and assess CI/KR within their jurisdictions. State homeland security advisors should work closely with DHS and the SSAs to ensure that data collection efforts are streamlined, coordinated, and reflect the most accurate data possible.
- The most current and accurate data are best known by CI/KR owners and operators themselves. Thus, as the owners and operators of the majority of the Nation's CI/KR, private sector entities are encouraged to be actively involved in the development and population of the NADB. Primarily through the voluntary provision of CI/KR information and industry-specific subject matter expertise, the private sector is playing an integral role in the expansion of the NADB.

3C.7 What Are the Plans for NADB Expansion?

The current NADB incorporates a flexible design to facilitate evolution, growth, and continued interconnectivity with additional databases and tools. Advancements will include integration with multiple commercial and Federal CI/KR databases, vulnerability assessment tools and libraries, intelligence and threat reporting databases, and geospatial tools into a single, integrated, Web-based portal.

DHS is developing the next-generation NADB with a more versatile platform to better support integration of DHS and SSA mission-specific applications and mission-specific databases. The goal of this effort is to create a national CI/KR inventory that more efficiently and effectively supports the implementation of NIPP risk management framework activities, including:

- Integration of vulnerability, consequence, and asset/system/network attribute data into a single portal interface to be used as the foundation for the NIPP risk assessment process;
- Access to threat data to support the development of asset, system, and network risk scores;

[37] The DHS/OIP taxonomy is the foundation for multiple DHS programs that focus on CI/KR, such as the NADB and the National Threat Incident Database, and should provide the foundation for the lexicon used in the SSPs. This common framework will allow more efficient integration and transfer of information, as well as a more effective analytical tool for making comparisons.

- Assessment and, if appropriate, prioritization of assets, systems, and networks across sectors and jurisdictions based on risk to promote the more effective allocation and use of available resources and to inform planning, threat response, and post-incident restoration actions at all levels of government and the private sector;
- Sharing of consistent information so that all partners involved in CI/KR protection operate from a common frame of reference;
- Acting as a primary information and integration hub for protective security needs throughout the country in support of DHS- and SSA-led activities;
- Supporting the efforts of law enforcement agencies during National Security Special Events and other high-priority security events; and
- Supporting the efforts of primary Federal agencies in responding to and recovering from major natural or manmade disasters.

Appendix 4: Organizing and Partnering for CI/KR Protection: Existing Coordination Mechanisms

The coordination mechanisms established under the NIPP serve as the primary means for coordinating CI/KR protection activities nationally. However, many other avenues exist for security partners to engage with each other and government at all levels to ensure that their efforts are fully coordinated in accordance with the principles outlined in the NIPP. The following table summarizes many of these available mechanisms.

Coordination	Mechanism	Description
Local to Local	Inter-Local Agreements	Cities and towns exchange information and cooperate on any number of projects. Inter-local agreements are a mechanism to do cooperatively anything that can be done as an individual municipality.
	Mutual-Aid Agreements	Established means through which one local government can offer assistance and another receive assistance in a time of disaster. These agreements cover logistics, deployment, liability, reimbursement, and many other issues. The intent is to provide assistance in the most efficient manner possible by coordinating the relevant terms and conditions in advance.
	County Commissioner Interaction	County commissioners provide leadership, services, and programs to meet the health, safety, and welfare needs of their citizens in an integrated, collaborative network.
Local to State	Committees, Commissions, and Boards	Local-to-State legislative- and regulatory-level interactions occur through State committees, commissions, and boards dealing with counter-terrorism, environmental, transportation, community development, retirement, insurance, and many other issues. Interactions also include coordination between the office of the Governor, homeland security advisor, Emergency Management Agency, and National Guard.
Local to Federal	Associations	National associations of local governments serve as a bridge between local elected officials and the Federal Government to ensure that the public safety and homeland security needs of localities are met. These organizations, such as the National League of Cities, the National Association of Counties, and the U.S. Conference of Mayors, work to ensure that Federal resources are appropriately targeted for disaster planning, mitigation, and recovery.
State to State	Intrastate Councils of Government	Councils of State Governments are regional councils that, by law, are political subdivisions of the State with the authority to plan and initiate needed cooperative projects; however, they do not have the power to regulate or tax because these authorities are exclusively assigned to cities and counties. A council's duties may include comprehensive planning for regional employment and training needs, criminal justice, economic development, homeland security, emergency preparedness, bioterrorism, 911 service, solid waste, aging, transportation, and rural development, among various others.
	Interstate or Regional Compacts (including those with cross-border entities)	States face issues that are not confined to geographical boundaries or jurisdictional lines. Interstate compacts are a mechanism that can be used to address sector interdependencies and coordinate protection of CI/KR. Compacts are organized in a number of ways: • Sector-based compacts focus on specific CI/KR resources that are shared or are interdependent across State boundaries (e.g., the Western Interstate Energy Compact); • Preparedness-focused compacts, such as the Interstate Mutual-Aid Compact, establish a means for participating jurisdictions to provide voluntary assistance to other States in response to an event that overwhelms the resources of individual State and local governments; and • Regional compacts provide a means for participating jurisdictions to coordinate activities within a specific geographical area that spans multiple States. These agreements, such as the Canadian River Compact, define the specific equities of each State within the particular region. For more information on interstate compacts, contact the National Center for Interstate Compacts: www.csg.org/programs/ncic/default.aspx.

Coordination	Mechanism	Description
State to Federal	Associations	Organizations such as the National Governors Association, National Conference of State Legislatures, and Council of State Governments represent the interests of States in the Federal policymaking process. State-level professional associations, such as the Association of State Drinking Water Administrators and the Association of State Water Pollution Control Administrators, also provide sector-specific coordination mechanisms. Additionally, these groups support State leaders by keeping their members informed of key Federal decisions that impact State government.
	State Liaison Offices	Some States have formed specific liaison offices in Washington, DC, to maintain awareness of Federal developments and ensure that their individual State perspective is represented in the Federal policymaking process. These offices report back regularly to their State's leadership and legislature regarding Federal issues of interest.
Federal to Federal	Memoranda of Understanding or Agreement	Agreements between two or more Federal departments and agencies to cooperate on a specific topic or initiative.
Private Sector to Government (all levels)	Public-Private Partnerships	Contractual agreement between a public agency (i.e., Federal, State, or local) and a private sector entity. Through this agreement, the skills and assets of each sector (public and private) are shared in delivering a service or facility for the use of the general public.
	Advisory Councils, Boards, and Commissions	In addition to the SCCs and ISACs, a variety of private sector organizations exist that focus on homeland security and CI/KR protection activities on a sector and geographical basis. These groups are made up of members of the public and subject matter experts, and provide advice and recommendations to governments at all levels.
	Associations	Myriad private sector associations exist that advocate on behalf of their members in the policymaking process at the Federal, State, and local levels. These groups are comprised of individuals or companies with common interests. Because of their ability to communicate with their members, private associations provide an effective means for government to provide information to the public and also learn the concerns of specific groups of security partners.

Appendix 5: Integrating CI/KR Protection as Part of the Homeland Security Mission

Appendix 5A: State, Local, and Tribal Government Considerations

State, local, and tribal efforts support the implementation of the NIPP and associated SSPs by providing a jurisdictional focus and enabling cross-sector coordination. The NIPP recognizes that there is not a one-size-fits-all approach to CI/KR protection planning at the State and local levels. Creating and managing a CI/KR protection program for a given jurisdiction entails building an organizational structure and mechanisms for coordination between government and private sector entities that can be used to implement the NIPP risk management framework. This includes taking actions within the jurisdiction to set security goals; identify assets, systems, and networks; assess risks; prioritize CI/KR across sectors; implement protective programs; and measure the effectiveness of risk-mitigation efforts. These elements form the basis of CI/KR protection programs and guide the implementation of relevant CI/KR protection-related goals and objectives outlined in State, local, and tribal homeland security strategies.

This appendix provides general guidance that can be tailored to unique jurisdictional characteristics, organizational structures, and operating environments at the State, local, and tribal levels.

The NIPP is structured to avoid redundancy and ensure coordination between State, local, and Federal CI/KR protection efforts. States or localities are encouraged to focus their efforts in ways that leverage Federal resources and address the relevant CI/KR sector's protection requirements in their particular areas or jurisdictions. This appendix outlines a basic framework to guide the development of CI/KR protection strategies, plans, and programs in coordination with the NIPP.

To align with the NIPP, State and local CI/KR protection plans and programs should explicitly address six broad categories regarding their CI/KR protection approach:

- CI/KR protection roles and responsibilities;
- Building partnerships and information sharing;

- Implementing the NIPP risk management framework;
- CI/KR data use and protection;
- Leveraging ongoing emergency preparedness activities for CI/KR protection; and
- Integrating Federal CI/KR protection activities.

5A.1 CI/KR Roles and Responsibilities

The NIPP outlines a set of broad roles and responsibilities for State, regional, local, and tribal entities (see chapter 2). State, regional, local, and tribal CI/KR protection plans (or elements addressing CI/KR in State or local homeland security plans or strategies) should describe how each jurisdiction intends to implement these roles and responsibilities. In particular, jurisdictions should consider and describe in their plans the following:

- Which offices or organizations in the jurisdiction perform the roles or responsibilities outlined in the NIPP or supporting SSPs;
- Whether gaps exist between the jurisdiction's current approach and those roles and responsibilities outlined in the NIPP or in an SSP, and how the gaps will be addressed;
- Whether any roles and responsibilities should be revised, modified, or consolidated to accommodate the unique operating attributes of the jurisdiction;
- How the jurisdiction will maintain operational awareness of the performance of the CI/KR protection roles assigned to different offices, agencies, or localities; and
- How the jurisdiction will coordinate its CI/KR protection roles and responsibilities with other jurisdictions and the Federal Government.

5A.2 Building Partnerships and Information Sharing

Effective CI/KR protection requires the development of partnerships, collaboration, and information sharing between government and private sector owners and operators. This includes maintaining awareness of CI/KR owner and operator concerns, disseminating relevant information to owners and operators, and maintaining processes for rapid response and decisionmaking in the event of a threat or incident involving CI/KR within the jurisdiction. To address partnership building, networking, and information sharing, State and local entities should determine whether the appropriate mechanisms for sharing information and networking with security partners are in place. If mechanisms are not established at all of the relevant levels, State and local entities should identify means for better coordinating and sharing information with security partners. Options to be considered and described in State, regional, local, and tribal CI/KR protection plans can include, but are not limited to:

- Ensuring collaboration with other government entities and the private sector using a process based on the partnership model outlined under the NIPP or an abbreviated form of the model addressing just those sectors that are most relevant to the jurisdiction;
- Instituting specific information-sharing networks, such as an information-sharing portal, for security partners in the jurisdiction. These types of networks allow owners and operators, and governmental entities to share best practices, provide a better understanding of sector and cross-sector needs, and inform collective decisionmaking on how best to utilize resources;
- Developing standing committees and work groups to discuss relevant CI/KR protection issues;

- Developing a regular newsletter or similar communications tool for CI/KR owners and operators on relevant CI/KR protection issues and coordination within the jurisdiction; and
- Participating in existing sector-wide and national information-sharing networks, including those offered by trade associations, ISACs, SCCs, and threat warning and alert notification systems.

The information-sharing approach for a given jurisdiction will vary based on CI/KR ownership, number and type of CI/KR sectors represented in the jurisdiction, and the extent to which existing mechanisms can be leveraged. The options presented above are merely a description of some available mechanisms that jurisdictions may consider as they develop the organization of their programs and document their processes in a CI/KR protection plan.

5A.3 Implementing the Risk Management Framework

The NIPP risk management framework described in chapter 3 provides a useful model for State, regional, local, and tribal jurisdictions to use in addressing CI/KR protection within the given jurisdiction. The process provides a risk-based approach that can help State and local entities to identify, prioritize, and protect CI/KR assets and systems within their jurisdictions. This process also allows State and local jurisdictions to enhance coordination with DHS and the SSAs in developing and implementing CI/KR protection programs. The following should be considered when developing CI/KR protection programs:

- What are the jurisdiction's goals and objectives for CI/KR protection? How do these goals relate to those of the NIPP and the SSPs that are relevant to the jurisdiction?
- What are the CI/KR assets, systems, networks, and functions within the jurisdiction or that impact the jurisdiction? Are there significant interstate or international dependencies or interdependencies? Are any of the assets, systems, or networks within the jurisdiction deemed to be nationally critical by DHS?
- Are risk assessments for CI/KR within the State being conducted or planned by DHS, SSAs, or owners and operators in accordance with the processes outlined in the NIPP? Is there a need for the jurisdiction to conduct additional or supplemental risk assessments? Do the methodologies for conducting risk assessments address the baseline criteria outlined in chapter 3?
- What are the CI/KR protection priorities within the jurisdiction? How do these priorities correlate with the national priorities established by the Federal Government? How do these priorities correlate with the ongoing CI/KR protection priorities established for each sector at the national level?
- What actions or initiatives are being taken within the jurisdiction to address CI/KR protection? How do these relate to the national effort?
- What types of metrics will be used to measure the progress of CI/KR protection efforts?

5A.4 CI/KR Data Use and Protection

States and other jurisdictions may employ a variety of means to collect CI/KR data or respond to CI/KR data requests. State, regional, local, and tribal plans should outline how the jurisdiction has organized itself to address CI/KR data use and protection. The following issues should be considered in developing the CI/KR protection plan:

- Will the jurisdiction maintain a comprehensive database of CI/KR in the State, region, or locality? How will the jurisdiction collect such information?

- How will sensitive data that may be in the possession of State, local, or tribal governments be legally and physically protected from public disclosure, and what safeguards will be used to control and limit distribution to appropriate individuals?
- Will data collection mechanisms be compatible and interoperable with the NADB to enable data sharing?
- How will the jurisdiction ensure that it is maintaining current information?
- Will data requests from the Federal Government for CI/KR data be channeled to the owners and operators through the States?
- Are there local legal authorities and policy directives related to data collection? Are these authorities adequate? If not, how will the jurisdiction address these issues?

5A.5 Leveraging Ongoing Emergency Preparedness Activities for CI/KR Protection

The emergency management capabilities of each State and local jurisdiction are an important component of improving overall CI/KR protection. States and localities should look to existing programs and leverage ways in which CI/KR protection can be integrated into ongoing activities. Areas to be considered when drafting a CI/KR protection plan include:

- Does the jurisdiction's exercise program account for CI/KR protection? If not, how will the State or locality incorporate CI/KR protection exercise scenarios to increase the level of preparedness?
- How do CI/KR protection efforts relate to initiatives outlined in the jurisdiction's hazard mitigation plan? How do various hazard modeling or ongoing mitigation efforts relate to the CI/KR protection initiatives?
- How will the jurisdiction share best practices, reports, or other output from emergency preparedness activities with CI/KR owners and operators?
- Have CI/KR owners and operators been invited to participate in exercise events, and are CI/KR owners and operators linked to existing warning or response systems?
- What existing education and outreach programs can be leveraged to share information with security partners regarding CI/KR protection?
- Are there other outreach or emergency management programs that should include a CI/KR component?

5A.6 Integrating Federal CI/KR Protection Activities

State-, local-, and tribal-level CI/KR protection programs should complement and draw on Federal efforts to the maximum extent possible to utilize risk management methodologies and avoid duplication of efforts.

State, local, and tribal efforts should consider the adequacy of DHS and SSA guidance and resources for their particular situation. For example:

- Are the existing criteria for risk analysis inclusive of levels of consequence that are of concern to the State or locality, or should the jurisdiction's criteria be expanded to include additional local assets?
- Are the self-assessment tools developed by DHS and the SSAs sufficient, or do these tools need additional tailoring to reflect local conditions?
- Are there additional best practices that should be shared among security partners?
- Are there additional authorities that need to be documented?

Appendix 5B: Recommended Homeland Security Practices for Use by the Private Sector

This appendix provides a summary of practices that may be adopted by private sector owners and operators to improve the efficiency and effectiveness of their CI/KR protection programs. The recommendations herein are based on best practices currently in use by various sectors and other groupings. The NIPP encourages private sector owners and operators to adopt and implement those practices that are appropriate and applicable at the specific sector enterprise and individual facility levels:

- **Asset, System, Network, and Function Identification:**
  - Incorporate the NIPP framework for the assets, systems, and networks under their control; and
  - Voluntarily provide CI/KR-related data to DHS to facilitate national CI/KR protection program implementation with appropriate information protections.
- **Assessment, Monitoring, and Reduction of Risks/Vulnerabilities**:
  - Conduct appropriate risk and vulnerability assessment activities using tools or methods that are rigorous, well-documented, and based on accepted practices in industry or government;
  - Implement measures to reduce risk and mitigate deficiencies and vulnerabilities corresponding to the physical, cyber, and human security elements of CI/KR protection;
  - Maintain the tools, capabilities, and protocols necessary to provide an appropriate level of monitoring of networks, systems, or a facility and its immediate surroundings to detect possible insider and external threats;
  - Develop and implement personnel screening programs to the extent feasible for personnel working in sensitive positions; and

- Manage the security of computer and information systems while maintaining awareness of vulnerabilities and consequences to ensure that systems are not used to enable attacks against CI/KR.

- **Information Sharing:**
  - Connect with and participate in the appropriate national, State, regional, local, and sector information-sharing mechanisms (e.g., HSIN-CS and the sector information-sharing mechanism);
  - Develop and maintain close working relationships with local (and, as appropriate, Federal, State, Territorial, and tribal) law enforcement and first-responder organizations relevant to the company's facilities to promote communications, with appropriate protections, and cooperation related to prevention, remediation, and response to a natural disaster or terrorist event;
  - Provide applicable information on threats, assets, and vulnerabilities to appropriate government authorities, with appropriate information protections;
  - Share threat and other appropriate information with other CI/KR owners and operators;
  - Participate in activities or initiatives developed and sponsored by relevant NIPP SCC or entity that provides the sector coordinating function;
  - Participate in, share information with (with appropriate protections), and support State and local CI/KR protection programs, including coordinating and planning with Local Emergency Planning Committees;
  - Collaborate with other CI/KR owners and operators on security issues of mutual concern; and
  - Use appropriate measures to safeguard information that could pose a threat and maintain open and effective communications regarding security measures and issues, as appropriate, with employees, suppliers, customers, government officials, and others.

- **Planning and Awareness**:
  - Develop and exercise appropriate emergency response, mitigation, and business continuity-of-operations plans;
  - Participate in Federal, State, local, or company exercises and other activities to enhance individual, organization, and sector preparedness;
  - Demonstrate continuous commitment to security and resilience across the entire company;
  - Develop an appropriate security protocol corresponding to each level of the HSAS. These plans and protocols are additive so that as the threat level increases for company facilities, the company can quickly implement its plans to enhance physical or cyber security measures in operation at those facilities and modify them as the threat level decreases;
  - Utilize National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, endorsed by DHS and Congress, when developing Emergency Response and Business Continuity-of-Operations Plans if the sector has not developed its own standard;
  - Document the key elements of security programs, actions, and periodic reviews as part of a commitment to sustain a consistent, reliable, and comprehensive program over time;
  - Enhance security awareness and capabilities through periodic training, drills, and guidance that involve all employees annually to some extent and, when appropriate, involve others such as emergency response agencies or neighboring facilities;

– Perform periodic assessments or audits to measure the effectiveness of planned physical and cyber security measures. These audits and verifications should be reported directly to the CEO or his/her designee for review and action;

– Promote emergency response training, such as the Community Emergency Response Team training offered by the U.S. Citizen Corps,[38] for employees;

– Consider including programs for developing highly secure and trustworthy operating systems in near-term acquisition or R&D priorities;

– Create a culture of preparedness, reaching every level of the organization's workforce, which ingrains in each employee the importance of awareness and empowers those with responsibilities as first-line defenders within the organization and community;

– As the organization performs R&D or acquires new or upgraded systems, consider only those that are highly secure and trustworthy;

– Encourage employee participation in community preparedness efforts, such as Citizen Corps, schools, Red Cross, Second Harvest, etc.;

– Work with others locally, including government, nongovernmental organizations, and private sector entities, both within and outside its sector, to identify and resolve gaps that could occur in the context of a terrorist incident, natural disaster, or other emergency;

– Work with the DHS to improve cooperation regarding personnel screening and information protection; and

– Identify supply chain and "neighbor" issues that could cause workforce or production disruptions for the company.

[38] The U.S. Citizen Corps is a national organization that brings citizen groups together and focuses the efforts of individuals through education, training, and volunteer service to help make communities safer, stronger, and better prepared to address the threats of terrorism, crime, public health issues, and disasters of all kinds. It works through a national network of State, local, and tribal Citizen Corps Councils that include leaders from law enforcement, fire, emergency medical, emergency management, volunteer organizations, local elected officials, the private sector, and other community stakeholders. More information is available on the internet at www.CitizenCorps.gov.

Appendix 6: Research and Development to Improve CI/KR Protection Capabilities

This appendix provides additional details on R&D programs and initiatives supporting the NIPP. It also includes details of R&D planning and programs undertaken in three areas: (1) those conducted under the NCIP R&D Plan; (2) those conducted by the SSAs and other agencies in support of requirements set forth in the President's physical and cyber security CI/KR strategies; and (3) those classified as Technology Pilot Programs, which develop technology-based solutions using more mature technology.

6.1 The National Critical Infrastructure Protection R&D Plan

As directed by HSPD-7, the Secretary of Homeland Security works with the Director of the OSTP, Executive Office of the President, to develop the annual NCIP R&D Plan.

The NCIP R&D Plan uses the three-step approach described below to direct the development of CI/KR protection-related technologies to meet existing and future requirements:

Step 1: Identify CI/KR Protection R&D Strategic Goals and Objectives

The NCIP R&D planning process identifies three long-term strategic goals and provides direction to the R&D community through a prioritized CI/KR protection agenda:

- **A common operating picture architecture** that will integrate CI/KR monitoring and support systems with data collection, processing, analysis, modeling, and simulation, including interdependencies and visualization capabilities, to provide real-time analysis and reports on the status and security of the Nation's CI/KR;

- **A next-generation Internet architecture** with designed-in security that is more secure than the existing Internet. The architecture will incorporate security and protection measures at all levels, from the basic hardware components through all layers of software, as an explicit design feature of this new network, rather than adding it later as a post-development patch; and
- **Resilient, self-diagnosing, self-healing systems** that, if attacked or damaged, can manage or contain the extent of the damage, continue to provide critical services, and adapt and self-heal damaged areas.

Step 2: Identify CI/KR Protection R&D Themes

The S&T needs for CI/KR protection programs fall into nine topical themes, or R&D areas, that cut across all CI/KR sectors:

- **Detection and Sensor Systems:** Selection, placement, and integration of systems to detect WMD intrusion, small arms, intent, humans (actors and victims), and disease outbreak. The research plans for certain sensors and detectors reside within several R&D communities, specifically for chemical, biological, radiological, nuclear, and explosive agents. The standards community also has a role in fostering interoperable sensor systems and establishing performance specifications.
- **Protection and Prevention Systems:** Devices, methods, and processes that prevent damage, disruption, or destruction of CI/KR. This theme involves layers of defensive measures that deter attackers, prevent entry, inhibit the use of weapons, and harden infrastructure.
- **Entry and Access Portals:** Devices, systems, and methods that control access to CI/KR. The types of portals include physical entryways and communications nodes. The objects of interest passing through portals include people, vehicles, goods, cargo and freight, electronic information, and communications. The enabling technologies include full life-cycle identity management, including biometric identification and automated identification strong authentication methods such as biometrics, radio frequency tags, sensor data, and x-ray interrogation systems.
- **Insider Threat Detection:** Profiling, detection, anticipation, and monitoring of activities of trusted persons or automated entities with access to a critical asset, system, or network, whether central or distributed. This theme focuses on detecting malicious intent, monitoring activities to identify anomalies and early indicators, and prevention and protection through real-time auditing of systems and layered measures to prevent malicious actions.
- **Analysis and Decision Support Systems:** Modeling, simulation and analysis, and decision support tools to analyze the complex systems and situations found in terrorist attack scenarios, including dependencies and interdependencies among sectors. This theme is of ubiquitous importance across sectors because CI/KR assets, systems, and networks are highly interdependent. Systems to be developed include risk-based prioritization and investment strategy aids; vulnerability assessment tools; modeling and simulation of sector operations, interconnectivity, and the consequences of attacks; and response planning tools to simulate scenarios and evaluate candidate responses.
- **Response, Recovery, and Reconstitution Tools:** Systems, devices, and processes that support first-responders and those building temporary and permanent replacement of damaged infrastructure, as well as the planning systems for all such efforts. Associated technologies include equipment to detect victims and assess safety hazards, simulation tools for response planning and training, and self-recovery design for cyber systems.
- **Emerging Threats and Vulnerabilities Analysis Aids:** Methods and processes that enable early discovery of emerging threats and vulnerabilities or the potential of adversaries to present new threats. Many emerging physical threats relate to changes in the lethality, detectability, or resistance to countermeasures of WMD agents. New cyber threats include those with the capability to attack a wide range of networks; new health threats include the emergence of infectious diseases, such as pandemic flu.

- **Advanced Infrastructure Architectures:** Use of new technology and associated designs that address current and future infrastructure needs with replacements that are inherently more secure (e.g., Internet contingency and SCADA system security). Greater inherent security can rely on automatic responses to attacks, self-healing features, and co-design of physical and cyber components that can prevent, respond to, or recover from attacks more quickly than current systems. Such improvements can have important dual-use benefits, with systems better able to respond to minor, but frequent, accidental events that degrade performance.
- **Human and Social Issues:** Research into behavioral issues related to victim response and CI/KR owner/operator actions to enhance understanding and decisionmaking during a terrorist event. The focus areas for this theme include coordination among government and private sectors, user-centered designs, the resiliency of commercial enterprises and the economy, and risk communications and management.

Step 3: Establish the NCIP R&D Technology Roadmap

The final step of the planning process involves the development of the NCIP R&D Technology Roadmap. Patterned after the technology roadmaps in wide use across U.S. industry, the roadmap provides a way for Federal managers such as DHS, OSTP, OMB, and the SSAs to coordinate infrastructure protection R&D, as well as a systematic approach to identify current technology investment plans, determine gaps, and outline the timeline for addressing unmet requirements.

6.2 Other R&D That Supports CI/KR Protection

Other R&D efforts, developed in accordance with the requirements set forth in the President's Physical and Cyber CI/KR Protection Strategies, that will be used to support CI/KR risk mitigation are discussed in this section. These requirements include:

- Ensure compatibility of communications systems with interoperability standards;
- Explore methods to authenticate and verify personal identity;
- Coordinate development of CI/KR protection consensus standards; and
- Improve technical surveillance, monitoring, and detection capabilities.

Examples of programs in each of these areas are discussed below to illustrate the potential benefits of such programs to security partners.

6.2.1 Ensure Compatibility of Communications Systems With Interoperability Standards

SAFECOM, a program in the DHS S&T Directorate, serves as the Federal umbrella to promote and coordinate initiatives among State, local, and tribal entities to improve first-responder communications through more effective and efficient interoperable wireless communications. SAFECOM's primary role is to work with Federal agencies and public safety personnel to define requirements and create standards, models, and solutions to help meet those requirements.

SAFECOM's role in standards development is to:

- Support existing or, where necessary, establish a voluntary consensus process that meets the current security environment, identifies and implements the needs and requirements of public safety, and maximizes flexibility and innovation; and
- Develop near-term tools that can maximize the efficiency of public safety technology, such as recommended models for statewide planning, criteria for creating governing bodies, standard operating procedures, grant guidance, and communications-specific exercise methodologies.

The following are key characteristics of SAFECOM's approach to facilitating the development of national voluntary consensus standards for public safety interoperable communications:

- Implements a practitioner-driven approach;
- Applies a comprehensive framework that utilizes a structured life-cycle approach that employs continuously evolving common grant guidance to assist communities in planning and implementing interoperability solutions;
- Integrates new and legacy systems using a "system of systems"; and
- Establishes industry and government partnerships.

6.2.2 Explore Methods to Authenticate and Verify Personal Identity

In coordination with a number of Federal agencies, DHS funds several R&D programs related to the authentication and verification of personal identity for the CI/KR workforce. Examples include research into the protection of physical infrastructure by authentication of network users, recommendations from the private security guard industry on legislative measures needed to achieve progress in the area of personnel surety (including enhanced capabilities for background checks on personnel with critical access), and advances in basic research. Another example is the DHS Office of National Capital Region Coordination initiative to establish partnerships with Federal, State, and local governments, as well as private sector organizations, to provide strong, machine-readable identity authentication for CI/KR response/support personnel in its region.

6.2.3 Coordinate Development of CI/KR Protection Consensus Standards

DHS worked with the American National Standards Institute and NIST to establish a Homeland Security Standards Panel that has been coordinating the development of consensus standards among the 280 different standards development organizations. An important product of this work was the standards supporting HSPD-12, which mandates reliable forms of identification issued by the Federal Government, as well as the identity-proofing guidance supporting the eAuthentication initiative.

6.2.4 Improve Technical Surveillance, Monitoring, and Detection Capabilities

Advances in surveillance, monitoring, and detection increase the Nation's ability to find threats in the making rather than responding to an attack after the fact. From an R&D perspective, advanced processing of digital video and other data collection methods is important in providing information to responsible security forces in a way that is reliable, practical, and fast. In cooperation with the United Kingdom, U.S. expertise has been brought to bear on reducing the amount of data that needs to be transmitted by extracting out only that information required for sophisticated analysis. Massive data storage capacity that is small and affordable is also nearing readiness for the market as a result of R&D investments by the government and private sectors. These advances make better use of the data collection capacity readily available, while providing information to security officials in a more actionable, focused manner.

In addition, the integration of biological, chemical, and radiological environmental and public health surveillance monitoring and detection capabilities, coupled with analysis tools, provides additional situational awareness and improves the ability of decisionmakers to determine appropriate courses of action in a WMD event.

6.3 Technology Pilot Programs

DHS identifies CI/KR protection needs common to certain types of assets, sectors, or high-risk jurisdictions in the course of conducting site assistance visits, buffer zone protection visits, and other vulnerability and risk assessments. In some situations, a technological development program is required to create or test the appropriate technological solution, and

the DHS S&T Directorate works closely with other relevant security partners to conduct a Technology Pilot Program. If the pilot program is successful, the technological solutions are then implemented in other locations where similar needs exist. The following descriptions of Technology Pilot Programs provide good examples of the capabilities that these programs can offer security partners:

6.3.1 National Capital Region Rail Security Corridor Pilot Project

This pilot project is designed to meet the needs of local law enforcement, first-responders, and the Federal Government while supplementing the existing security measures of freight rail operations in the Washington, DC, area. This pilot project seeks to address security challenges surrounding rail infrastructure and freight traffic through large cities while maintaining fluid rail operations. The pilot project components include a "virtual security fence" consisting of approximately 200 high-resolution fixed cameras, the use of radio frequency identification scanners, and virtual gates for chemical and radiological detection. Data from the fence and the gates will be encrypted and transmitted simultaneously to multiple locations, such as the U.S. Capitol Police, U.S. Secret Service, the rail corridor's owner/operator, and other applicable Federal or local agencies.

6.3.2 Constellation Automated Critical Asset Management System

Constellation/ACAMS, developed through a partnership between DHS and the City and County of Los Angeles as part of the Operation Archangel CI/KR protection program, encompasses automated systems, tools, resources, and related training to enable the protection of CI/KR located in major urban areas. Constellation/ACAMS enables planning for, responding to, and recovering from catastrophic incidents. As such, it focuses on the unique requirements and information needs of first-responders. It possesses a complete reporting capability to answer both local and national data calls on critical assets, including information on location, size, key contacts, types of hazardous materials on site, and vulnerability assessments. It also provides for the automatic generation of BZPP and pre-incident operational plans for local police and first-responder use.

6.3.3 South Florida Coastal Surveillance Prototype Test Bed

The DHS S&T Directorate and the USCG planned and funded the South Florida Coastal Surveillance Prototype Test Bed, a port and coastal surveillance prototype in the Port Everglades, Miami, and Key West areas. The evolutionary prototype provides an initial immediate coastal surveillance capability in a high-priority area that:

- Offers the means to develop and evaluate a concept of operations in a real-world environment;
- Implements and tests interoperability among DHS and DOD systems and networks such as the U.S. Navy/USCG Joint Harbor Operations Center;
- Tests and evaluates systems and operational procedures; and
- Becomes the design standard for follow-on systems in other areas and integration with wider area surveillance systems.

Homeland
Security